Virtual Engine Toolkit
User Guide v1.4

© 2013 Virtual Engine Limited. All Rights Reserved.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Virtual Engine Limited.

If you have any questions regarding your potential use of this material, contact:

Website: http://virtualengine.co.uk/
E-mail: info@virtualengine.co.uk

Trademarks

Other trademarks and registered trademarks used in this guide are property of their respective owners.

Disclaimer

The information in this document is provided in connection with Virtual Engine products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Virtual Engine products.

EXCEPT AS SET FORTH IN VIRTUAL ENGINE'S TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, VIRTUAL ENGINE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL VIRTUAL ENGINE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF VIRTUAL ENGINE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Virtual Engine makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Virtual Engine does not make any commitment to update the information contained in this document.

VET User Guide v1.4.docx
Updated – 01/08/2013
Version – 1.4

License Agreement

Please read the terms and conditions of this license agreement (the "License") before installing the computer software (the "Software"). By installing and using the Software you accept and agree to the terms of this License. This License constitutes the entire agreement concerning the Software between you and Virtual Engine Limited and it supersedes any prior proposal or representation. If you do not agree with these terms and conditions, promptly de-install the Software

The term "Software" includes, and these terms and conditions also apply to, any updates, modifications and upgrades to the Software that you may receive from time to time.

1. License Grant

This License permits you to use any number of copies of the Software on your devices. The enclosed documentation ("Documentation") may not be copied. You agree that you will not sublicense, assign, transfer, distribute, pledge, lease, rent or share your rights under this License except with prior written permission from Virtual Engine Limited. You agree that you will not modify, adapt or translate, or disassemble, decompile, reverse engineer or otherwise attempt to discover the source code of the Software.

2. Virtual Engine's Rights

You acknowledge and agree that the Software and Documentation (the "Licensed Products") are proprietary products of Virtual Engine Limited under international copyright law and disclosed to you by Virtual Engine Limited in confidence. You shall take all reasonable steps to safeguard the Licensed Products. Virtual Engine Limited owns and retains all copyright, trademark, trade secret and other proprietary rights in and to the Licensed Products. This License conveys to you only a non-exclusive and limited right of use, revocable in accordance with the terms and conditions of this License.

3. Exceptions to Warranties; Disclaimers

EXCEPT FOR THE ABOVE EXPRESS LIMITED WARRANTY, VIRTUAL ENGINE LIMITED DISCLAIMS ANY AND ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR PARTICULAR PURPOSE. Virtual Engine Limited does not warrant that the Software, its use, operation or your ability to use the Software will be uninterrupted or error-free or that all Software errors will be corrected. The warranty set forth above shall not apply to any defect or problems caused by any defect in any hardware or software used in combination with the Software, or use of the Software in execution environments not specified in the Documentation. Virtual Engine Limited does not warrant that the Software or service will meet your requirements or that the operation of the Software will be uninterrupted or error free.

4. Limitations of Liability

In no event shall Virtual Engine Limited be liable for any damages to you or any other party whether arising out of contract or from tort including loss of data, profits or business or other special, incidental, exemplary or consequential damages, even if Virtual Engine Limited has been advised of the possibility of such loss or damages. Virtual Engine Limited's cumulative liability shall not exceed the license fee paid, if any, for use of this Software and Documentation. This section shall survive termination of this License.

5. Termination

This agreement is in effect until terminated. You may terminate the agreement at any time by destroying all copies of the Software and Documentation and erasing any copies on storage media. The agreement also terminates if you fail to comply with any terms and conditions of this agreement. In such event, you agree to destroy and erase all copies of the Software and Documentation, and Virtual Engine Limited will be entitled to all remedies in accordance with applicable law.

6. Data Collection

Virtual Engine Limited has the capability to monitor your usage of the Software to collect and aggregate certain technical data and related information about your use of the Software without any reference to the specific user-source of the data or information, and such collection and aggregation activities will be done in a manner that does not personally identify you. Virtual Engine Limited anticipates that its use of such data and information with help Virtual Engine Limited to improve its products and/or services to you. Data collected will not be shared with any third party companies.

7. General

This agreement shall be governed by the laws of the United Kingdom.

8. Contact

For further information, e-mail support@virtualengine.co.uk

Contents

Introduction 6

Guide Overview 6

About Virtual Engine 6

What's New 6

Prerequisites 6

VET Basics 7

VET Options 8

Access Control ..... **Error! Bookmark not defined.**

RES Workspace Manager Wizards 10

Importing Building Blocks into RES Workspace Manager 10

RES Workspace Manager GUIDs 11

Access Control Defaults 12

.CSV Conversion Wizard 12

Importing Active Directory Printers 17

Importing Active Directory Site Definitions 20

BBSpinner 24

Using BBSpinner 25

Convert POLs 27

Locating Group Policy Object GUIDs 27

Converting the REGISTRY.POL File 28

Importing GPOs Directly from Active Directory 29

Requirements 29

Running the Conversion Wizard 29

Merge ADMs and Merge ADMXs 35

ADMX File Format 35

Merging ADMs/ADMXs 35

GUIDs Locator 36

.ONCE File Locations 36

Retrieving RunOnce GUIDs 37

Profile Update Utility 38

The PuU Interface 39

Adding/Removing Profiles 39

Adding/Removing Registry Files 40

Ad-hoc Editing of Registry Files 40
Backup Options 41
Windows ActiveSetup keys 41
Deleting Profile Update Logs 42
Enabling Windows Aero Themes 42
International and Regional Options 43
Updating Profiles 44
Job Execution Tool 45
JET 45
Installation 45
JET Configuration 45
JETCMD 49
Installation 49
Usage 49
Passing Parameters 50
Verbose Logging 50
JETPWD 51
Installation 51
Usage 51
WSUS Integration Management Pack 52
Installation 53
Usage 53
Reboots 53
Appendix A – Group Policy Migration 54
Security Filtering 54

Introduction

Welcome to the Virtual Engine Toolkit User Guide. This section introduces Virtual Engine, its services and product offerings.

Guide Overview

The Virtual Engine Toolkit User Guide details how to utilise the Virtual Engine Toolkit (or VET) and included Profile Update Utility (PuU), Job Execution Tool (JET), JETCMD, JETPWD and WSUS Integration Management Pack (WiMP).

If you have any comments, suggestions or corrections please contact support@virtualengine.co.uk.

About Virtual Engine

Virtual Engine Limited is a privately held company in the United Kingdom and provides virtualisation consultancy and training services. In depth knowledge of desktop virtualisation, user environment management and desktop migration enables Virtual Engine partners to leverage highly skilled resources and project management expertise where required.

What's New

None. This is a maintenance release.

Prerequisites

Microsoft .NET Framework 4.0 (Full or Client Profile)

The Virtual Engine Toolkit has been designed and written using modern coding techniques, as such the Microsoft .NET Framework is required to allow the application to function correctly. The VET, PuU, JET, JETCMD and JETPWD components are reliant upon the Microsoft .NET Framework 4.0.

Note

The WSUS Management Integration Pack (WiMP) **does not** have any requirements or dependencies upon the Microsoft .NET Framework.

Microsoft Group Policy Manager Console (GMPC)

The Virtual Engine Toolkit references the Group Policy Management Console Class Library, therefore the GPMC needs to be installed on the machine running VET.

Note

The Job Execution Tool (JET), JETCMD and JETPWD **DO NOT** require the GPMC to be installed.

Active Directory Domain Membership

For the Virtual Engine Toolkit to use the Group Policy Management Console Class Library, the machine running VET must be joined to an Active Directory Domain.

Copyright © 2008 – 2013 Virtual Engine Limited

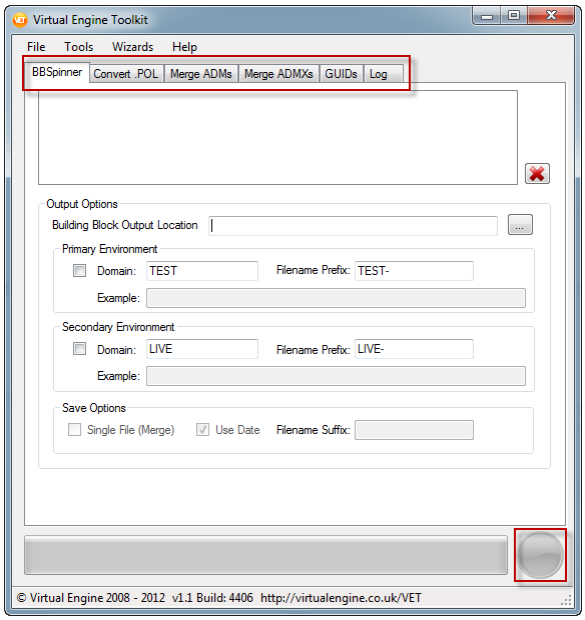
VET Basics

The Virtual Engine Toolkit is essentially a collection of tools for managing and/or implementing user environment management (UEM) products, e.g. RES Workspace Manager or AppSense Environment Manager.

Each tool typically has its own tab within the VET interface, although the Profile Update Utility, Job Execution Tool and Job Execution Tool Command are supplied as a separate executables.

Depending on which tab is selected, the input requirements for the tool will vary. When all required information has been completed successfully, the orange "orb" will become enabled. Clicking the orb will perform the actions specified by the currently selected tab.

Figure 1 - The VET Interface



The only exception to this is the ***Log*** tab which provides logging and diagnostic information of all actions performed. The log information can be copied/pasted and can also be saved to a text file via the ***File > Save Log File As*** menu option. This information is typically used by Virtual Engine Support to help debug any inconsistencies. When the Log tab is selected the VET button will always be greyed out/unavailable.

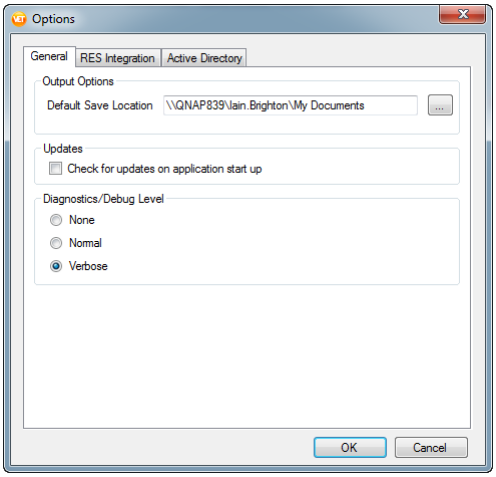
If you wish to clear the log windows, you can click the ***Tools > Clear Log File*** menu option at any time.

Copyright © 2008 – 2013 Virtual Engine Limited

VET Options

Throughout the VET interface and wizards, certain fields are prepopulated and these defaults can be changed as required. To access the default options and settings click the ***Tools > Options*** menu option.

Figure 2 - General Options

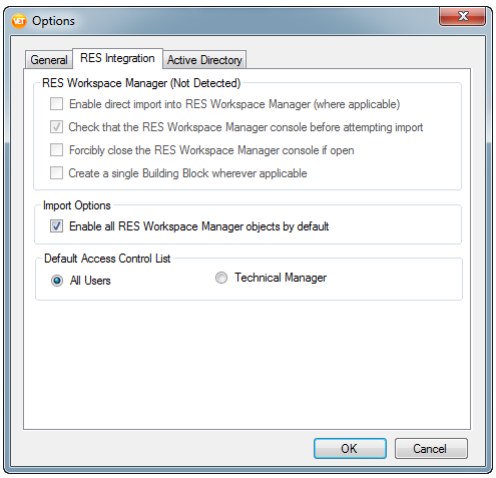


The default location used by VET for saving files is the current user's My Documents location. You can change this location by specifying a new location in the ***Default Save Location*** text box or by browsing to the desired folder.

Virtual Engine releases application updates and bug fixes from time-to-time and VET will automatically check for available updates. If you wish to disable this functionality ensure that the ***Check for updates on application start up*** is unchecked.

All actions performed by VET will be logged in the ***Log*** tab. The level of detail is configured in the ***Diagnostics/Debug Level*** option. If you wish to alter the level of logging, select the desired level here.

Figure 3 - RES Integration Options


Options
General
RES Integration
Active Directory
RES Workspace Manager (Not Detected)
Enable direct import into RES Workspace Manager (where applicable)
Check that the RES Workspace Manager console before attempting import
Forcibly close the RES Workspace Manager console if open
Create a single Building Block wherever applicable
Import Options
Enable all RES Workspace Manager objects by default
Default Access Control List
All Users
Technical Manager
OK
Cancel

The default RES Workspace Manager building block settings are located on the ***RES Integration*** tab in the ***Options*** window. If the RES Workspace Manager console is detected on the device that VET is

Copyright © 2008 – 2013 Virtual Engine Limited

running on, you can change the default import behaviour for any generated building blocks into RES Workspace Manager. To enable this ability by default, check the ***Enable direct import into RES Workspace Manger (where applicable)*** option. If this option is disabled and the RES Workspace Manager console is detected, you will have the ability to manually override this behaviour where possible.

The default import, activation and Access Control options are covered in the **Importing Building Blocks into RES Workspace Manager** and **RES Workspace** Manager GUIDs

Each RES Workspace Manager object has an associated globally unique identifier or GUID. This GUID is automatically generated when manually creating objects within the RES Workspace Manager console. If a RES Workspace Manager building block file is generated, the GUID is also stored.

If the object GUID in a building block matches an object within the RES Workspace Manager database when importing, the original item will be overwritten or updated. If the GUIDs are different then a duplicate object is created within the RES Workspace Manager database.

By default all objects imported by VET from Active Directory will utilise the GUID already present in Active Directory. This ensures that if the AD Sites, AD Printers or GPOs are imported and the wizard is run again, the GUIDs remain exactly the same. This ensures that, for example, new Active Directory sites created can be imported by re-running the wizard and it will not create duplicate objects in the RES Workspace Manager database.

Note

Deletions from Active Directory will not be reflected in any building block files and will need to be manually removed from the RES Workspace Manager database.

Note

The .CSV file conversion wizard generates GUIDs on the fly and therefore, re-running the wizard will generate different GUIDs every time.

Access Control

Only integrated (Windows) authentication for connecting to Active Directory. The option to manually specify connection information has been deprecated from this release (to support migration of GPO OU/site links and GPO security filtering.

Copyright © 2008 – 2013 Virtual Engine Limited

RES Workspace Manager Wizards

The Virtual Engine Toolkit can now convert .CSV files and Active Directory objects into RES Workspace Manager building block files. This enables IT administrators to quickly transition existing infrastructures to RES Workspace Manager for management whilst utilising existing information and/or configurations to aid in deployment. Any building blocks created by VET can also be directly imported into RES Workspace Manager from the conversion wizards[1].

The .CSV import wizard allows you to convert drive mappings, printers, file security authorisations and environment variable definitions listed in either comma separated (.CSV) or tab separated (.TSV) formats into RES Workspace Manager building block files.

It is also possible to convert Active Directory published printers, Active Directory site definitions and Group Policy Objects into building block files. Group Policy Objects can be converted to registry (.REG) files and RES Workspace Manager building blocks and this process is covered in the **Convert POLs** section.

Importing Building Blocks into RES Workspace Manager

The Virtual Engine Toolkit can directly import RES Workspace Manager building blocks into the RES Workspace Manager console. Throughout the various wizards, the ***Import into RES Workspace Manager Now*** window will be displayed as necessary.

Figure 4 – RES Workspace Manager Import Options

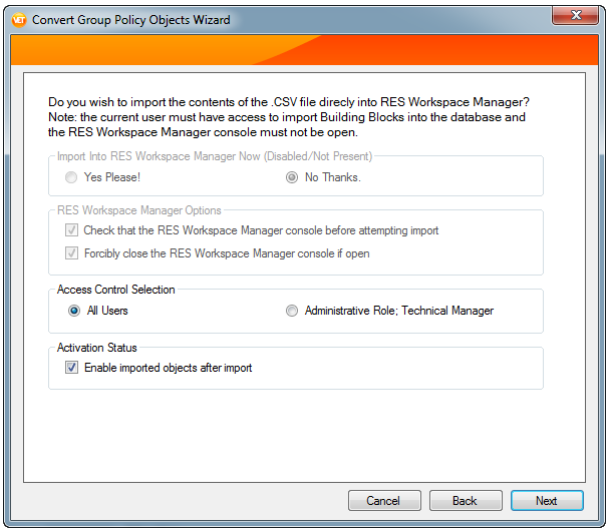

Convert Group Policy Objects Wizard
Do you wish to import the contents of the .CSV file direcly into RES Workspace Manager?
Note: the current user must have access to import Building Blocks into the database and the RES Workspace Manager console must not be open.
Import Into RES Workspace Manager Now (Disabled/Not Present)
Yes Please!
No Thanks.
RES Workspace Manager Options
Check that the RES Workspace Manager console before attempting import
Forcibly close the RES Workspace Manager console if open
Access Control Selection
All Users
Administrative Role; Technical Manager
Activation Status
Enable imported objects after import
Cancel
Back
Next

Figure 4 – RES Workspace Manager Import Options shows an example of these options. If the RES Workspace Manager integration is enabled, then the wizards will allow you to directly import any generated building blocks directly into the RES WM console.

Note

Directly importing RES Workspace Manager building blocks requires the RES Workspace Manager console (or full RES Workspace Manager agent) to be installed on the machine running VET.

[1] The RES Workspace Manager management console must be loaded onto the computer running VET.

Copyright © 2008 – 2013 Virtual Engine Limited

If the RES Workspace Manager console is not detected or the RES Workspace Manager integration is disabled, all the options will be greyed out.

When you see this option and you wish to directly import the generated building blocks into RES Workspace Manager, ensure that the ***Yes Please!*** option is selected. If you do not wish to import the building blocks then select the ***No Thanks*** option instead.

When importing RES Workspace Manager building blocks via the Virtual Engine Toolkit, the RES Workspace Manager console cannot be running. VET provides the ability to check that the console is not open and by default the ***Check that the RES Workspace Manager console before attempting import*** option is enabled. If required, this can be deselected.

The ***Forcibly close the RES Workspace Manager console if open*** option will automatically attempt to close the RES Workspace Manager console if it running to ensure the import process completes successfully.

Note

If the import process fails due to the console being open or it cannot be closed successfully, the resulting building blocks can always be imported manually.

When creating the RES Workspace Manager building blocks you may or may not want all the resulting objects to be automatically enabled. The ***Enable the imported objects after import*** option permits you to flag whether the generated objects are enabled or disabled by default. If the ***Enable imported objects after import*** is checked then all objects will be enabled in RES Workspace Manager. If the ***Enable objects after import*** checkbox is unchecked then all objects will be disabled in RES Workspace Manager and can be manually enabled as necessary.

RES Workspace Manager GUIDs

Each RES Workspace Manager object has an associated globally unique identifier or GUID. This GUID is automatically generated when manually creating objects within the RES Workspace Manager console. If a RES Workspace Manager building block file is generated, the GUID is also stored.

If the object GUID in a building block matches an object within the RES Workspace Manager database when importing, the original item will be overwritten or updated. If the GUIDs are different then a duplicate object is created within the RES Workspace Manager database.

By default all objects imported by VET from Active Directory will utilise the GUID already present in Active Directory. This ensures that if the AD Sites, AD Printers or GPOs are imported and the wizard is run again, the GUIDs remain exactly the same. This ensures that, for example, new Active Directory sites created can be imported by re-running the wizard and it will not create duplicate objects in the RES Workspace Manager database.

Note

Deletions from Active Directory will not be reflected in any building block files and will need to be manually removed from the RES Workspace Manager database.

Copyright © 2008 – 2013 Virtual Engine Limited

Note

The .CSV file conversion wizard generates GUIDs on the fly and therefore, re-running the wizard will generate different GUIDs every time.

Access Control Defaults

The .CSV Conversion Wizard does allow for users and groups to be mapped to the RES Workspace Manager objects that it creates. For this process to work successfully, you need to ensure that group names are included within the source .CSV file and that multiple groups are separated by semicolons (;).

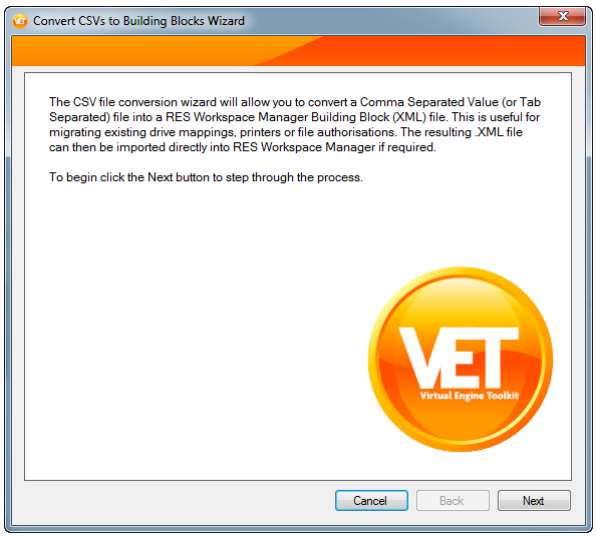
If Access Control mappings are defined in the .CSV Conversion Wizard, a default NetBIOS domain name will need to be specified to ensure that the mappings are created correctly, i.e. if group names are not listed in the <DOMAIN>\<GROUPNAME> format within the source file.

.CSV Conversion Wizard

When migrating to RES Workspace Manager it is often desirable to import existing objects definitions from existing sources rather than manually recreate them from scratch. Fortunately, the Virtual Engine Toolkit enables existing definitions of drive mappings, printers and environment variables to be converted to RES Workspace Manager building blocks. It is also possible to convert file authorisation lists from other security products. Template CSV files have been included as part of the Virtual Engine Toolkit installation to help understand the format the CSV files should take; these can be found in the ***CSV Templates*** folder under the Virtual Engine Toolkit installation folder.

To start the CSV Conversion wizard click the ***Wizards > RES Workspace Manager > Import CSV Files*** in the VET menu bar.

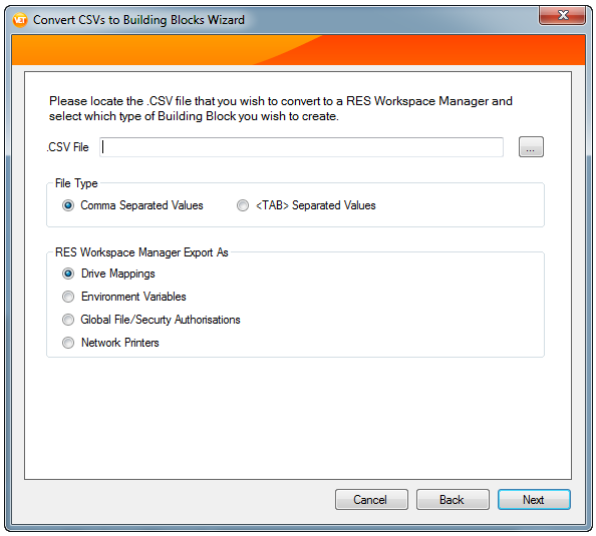
Figure 5 - CSV Conversion Wizard


Convert CSVs to Building Blocks Wizard
The CSV file conversion wizard will allow you to convert a Comma Separated Value (or Tab Separated) file into a RES Workspace Manager Building Block (XML) file. This is useful for migrating existing drive mappings, printers or file authorisations. The resulting .XML file can then be imported directly into RES Workspace Manager if required.
To begin click the Next button to step through the process.
VET
Virtual Engine Toolkit
Cancel
Back
Next

Click ***Next*** after you have read the introductory text.

Copyright © 2008 – 2013 Virtual Engine Limited

Figure 6 - CSV File Selection


Convert CSVs to Building Blocks Wizard
Please locate the .CSV file that you wish to convert to a RES Workspace Manager and select which type of Building Block you wish to create.
.CSV File
File Type
Comma Separated Values
<TAB> Separated Values
RES Workspace Manager Export As
Drive Mappings
Environment Variables
Global File/Security Authorisations
Network Printers
Cancel
Back
Next

For the wizard to convert a CSV file you need to tell it what .CSV file you wish to convert, what type of CSV file it is and which type of RES Workspace Manager building block file you create.

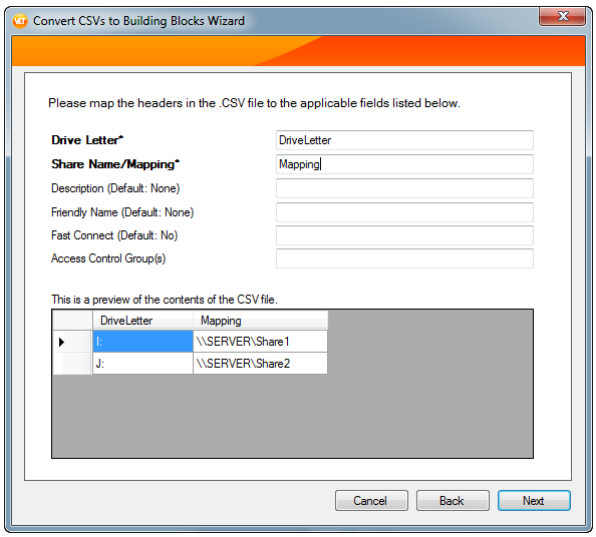
To select the source file that you want to convert either enter the full path to the file in the ***.CSV File*** textbox or utilise the browse button to locate the file.

The wizard also needs to know whether the delimiter in the text file is a comma or a tab character. If the source file is comma-delimited check the ***Comma Separated Values*** checkbox. If the source file is tab-delimited, ensure you select the ***<TAB> Separated Values*** checkbox.

Each type of RES Workspace Manage object you wish to create has different mapping fields. Therefore, it is important to select the correct destination object type. Ensure that you select the relevant object type in the ***RES Workspace Manager Export As*** selection.

Once ready to proceed and load the .CSV file, click the ***Next*** button.

Figure 7 - CSV Object Mapping



The .CSV file is loaded into the preview window so that you can see the detected column headings

Copyright © 2008 – 2013 Virtual Engine Limited

and values to specify the correct mapping. Figure 7 shows a sample .CSV file containing the drive letter and target mapped successfully.

Note

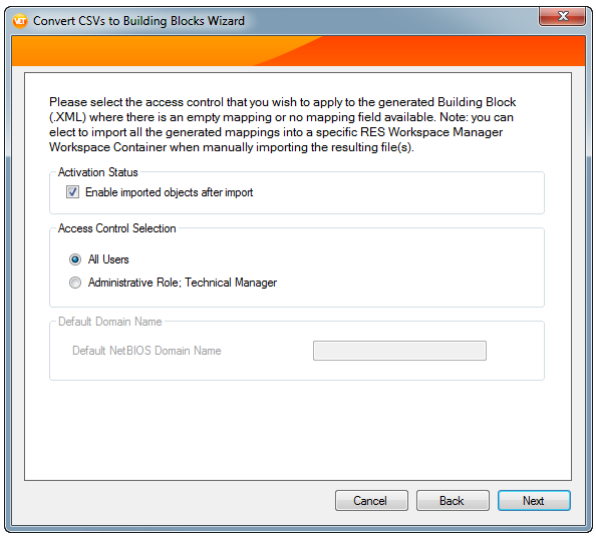
If the mapping fields are listed incorrectly, confirm that the correct file type has been selected, i.e. comma-separated or tab-separated and try again.

Depending on which RES Workspace Manager object type has been selected, the wizard will display differing columns for mapping to the .CSV file contents. The entries in **bold** and marked with an asterisk (*) are required for the wizard to convert the .CSV file and must be completed. Other optional columns are listed and can be mapped. If no mapping is specified for the optional components the listed defaults will be used.

To map column headings in the .CSV to the relevant RES Workspace Manager object, enter the listed column heading into the relevant textbox. In Figure 7, the ***DriveLetter*** column heading has be entered in the ***Drive Letter**** textbox. This configuration indicates that the DriveLetter column will be read from the CSV file (I: and J: in this instance) and used as the drive letter within RES Workspace Manager. Likewise, the ***Mapping*** column heading has been mapped to the ***Share Name/Mapping**** text box.

After you have mapped all the mandatory column headings and any optional headings, click the ***Next*** button.

Figure 8 - Activation Status and Access Control


Convert CSVs to Building Blocks Wizard
Please select the access control that you wish to apply to the generated Building Block (.XML) where there is an empty mapping or no mapping field available. Note: you can elect to import all the generated mappings into a specific RES Workspace Manager Workspace Container when manually importing the resulting file(s).
Activation Status
Enable imported objects after import
Access Control Selection
All Users
Administrative Role; Technical Manager
Default Domain Name
Default NetBIOS Domain Name
Cancel
Back
Next

If you wish to have the resulting RES Workspace Manager objects enabled when imported into the RES Workspace Manager console, ensure that the ***Enable imported objects after import*** is selected. Unchecking this option will disable the imported objects within the RES Workspace Manager console.

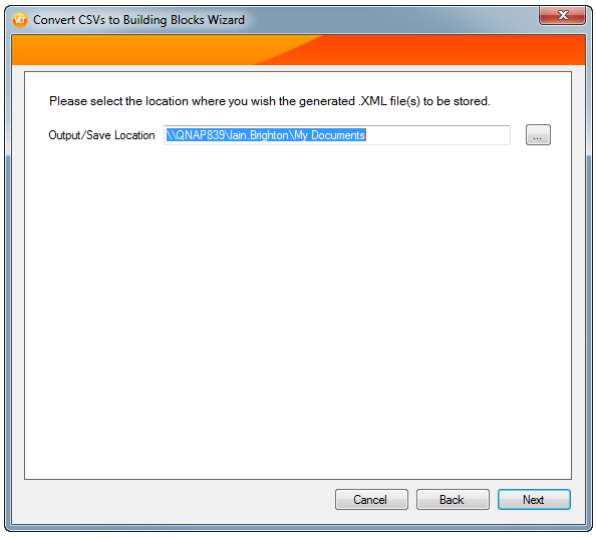
If no Access Control mapping has been defined you will need to select a default entry that is configured in the building block file. If you wish all users to be granted access to the objects, ensure that the ***All Users*** option is checked. If this isn't desirable, ensure that ***Administrative Role; Technical Manager*** is selected instead.

Copyright © 2008 – 2013 Virtual Engine Limited

If you define an Access Control mapping, then the ***Default Domain Name*** option will be enabled. Enter the default domain name to use when mapping the group names. This is required as RES Workspace Manager needs a domain name listed in its access control entries.

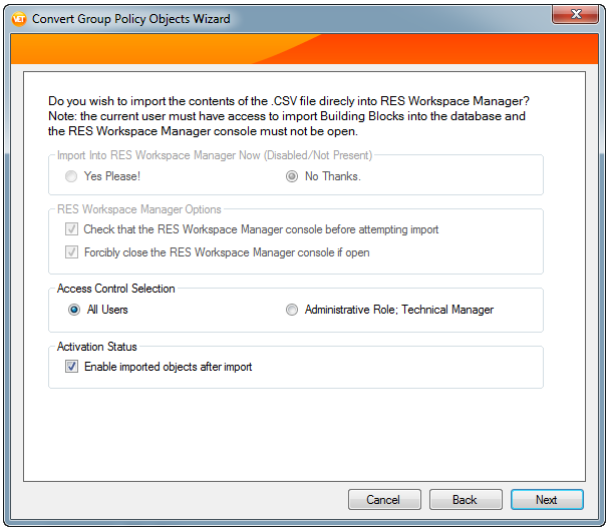
Once all the correct options have been selected, click the ***Next*** button to continue.

Figure 9 - CSV/XML Save Location



The default save location will be displayed and the resulting .XML file will be placed in this location. If you wish to change the save location update the ***Output/Save Location*** textbox or use the browse button. Once complete, click the ***Next*** button.

Figure 10 - RES Workspace Manager Import


Convert Group Policy Objects Wizard
Do you wish to import the contents of the .CSV file direcly into RES Workspace Manager?
Note: the current user must have access to import Building Blocks into the database and
the RES Workspace Manager console must not be open.
Import Into RES Workspace Manager Now (Disabled/Not Present)
Yes Please!
No Thanks.
RES Workspace Manager Options
Check that the RES Workspace Manager console before attempting import
Forcibly close the RES Workspace Manager console if open
Access Control Selection
All Users
Administrative Role; Technical Manager
Activation Status
Enable imported objects after import
Cancel
Back
Next

If you wish to import the generated building blocks directly into the RES Workspace Manager console click the ***Yes Please!*** option. If the options are greyed out then the RES Workspace Manager console has not been detected or the integration has been disabled. For more information on the RES Workspace Manager integration and options please refer to the **Importing Building Blocks into RES Workspace Manager** section.

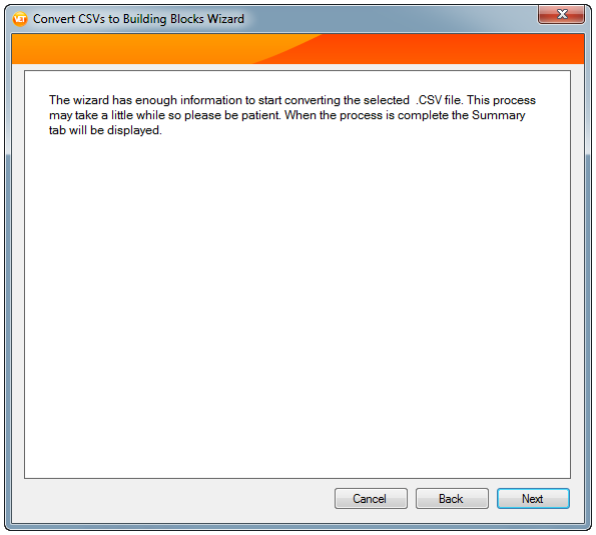
Copyright © 2008 – 2013 Virtual Engine Limited

The default access control defined within the building block can either be set to ***All Users*** or ***Administrative Role; Technical Manager***. Select the appropriate option in the ***Access Control Selection*** section.

If you wish the resulting RES Workspace Manager objects to be enabled after importing, ensure the ***Enable imported objects after import*** checkbox is selected. If you want them disabled, ensure it is unchecked.

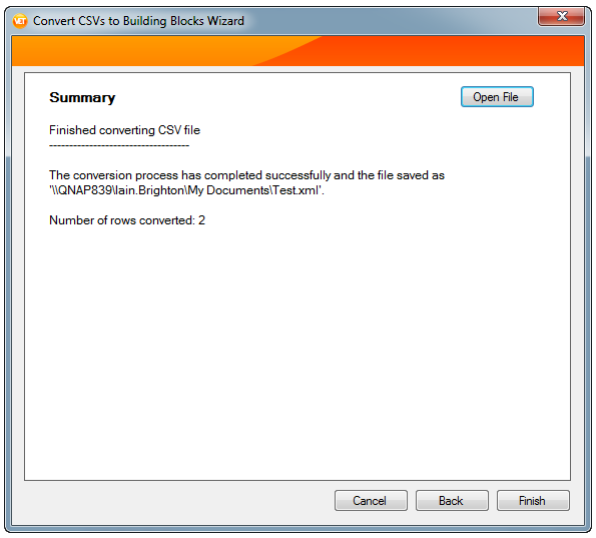
Click the ***Next*** button to proceed.

Figure 11 - CSV Conversion Ready


Convert CSVs to Building Blocks Wizard
The wizard has enough information to start converting the selected .CSV file. This process may take a little while so please be patient. When the process is complete the Summary tab will be displayed.
Cancel
Back
Next

If all options have been completed and configured correctly, the wizard will inform you it's ready to perform the conversion and import (if selected). Click the ***Next*** button to start the process.

Figure 12 - CSV Conversion Summary



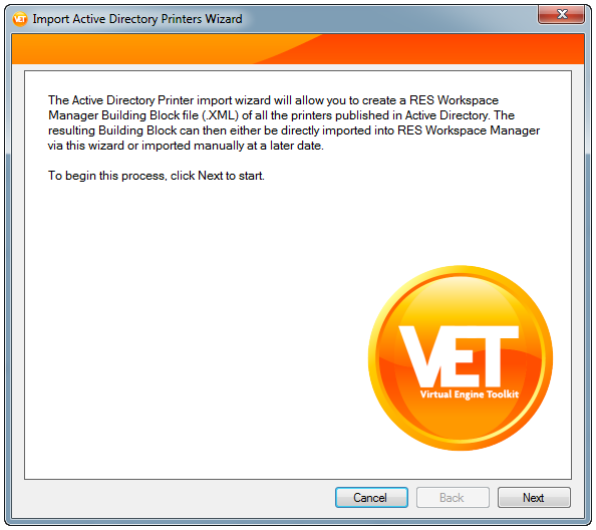
Once the conversion/import process is complete the summary screen will be displayed detailing the output file and location. If you wish to open the resulting .XML file, click the ***Open File*** button. To close the wizard click the ***Finish*** button.

Copyright © 2008 – 2013 Virtual Engine Limited

Importing Active Directory Printers

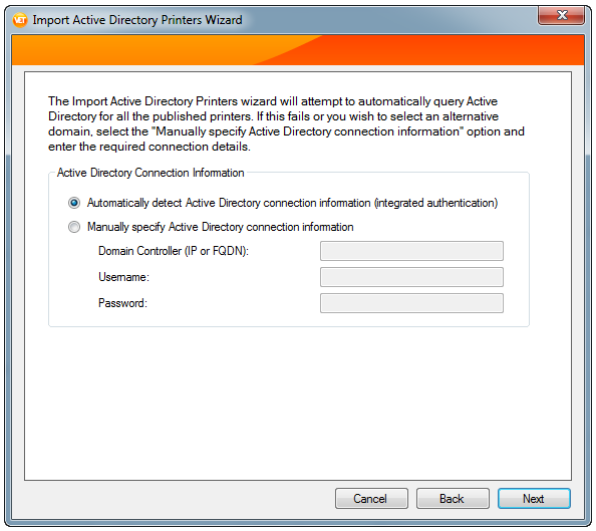
All published printers in Active Directory can be exported to a RES Workspace Manager building block file with the ***Import Active Directory Printers Wizard***. To launch the wizard click the ***Wizards > RES Workspace Manager > Import AD Printers*** menu option and the wizard should start.

Figure 13 - Import AD Printers Wizard


Import Active Directory Printers Wizard
The Active Directory Printer import wizard will allow you to create a RES Workspace Manager Building Block file (.XML) of all the printers published in Active Directory. The resulting Building Block can then either be directly imported into RES Workspace Manager via this wizard or imported manually at a later date.
To begin this process, click Next to start.
VET
Virtual Engine Toolkit
Cancel
Back
Next

After reading the introductory information , click the ***Next*** button to proceed

Figure 14 - AD Connection Information


Import Active Directory Printers Wizard
The Import Active Directory Printers wizard will attempt to automatically query Active Directory for all the published printers. If this fails or you wish to select an alternative domain, select the "Manually specify Active Directory connection information" option and enter the required connection details.
Active Directory Connection Information
Automatically detect Active Directory connection information (integrated authentication)
Manually specify Active Directory connection information
Domain Controller (IP or FQDN):
Username:
Password:
Cancel
Back
Next

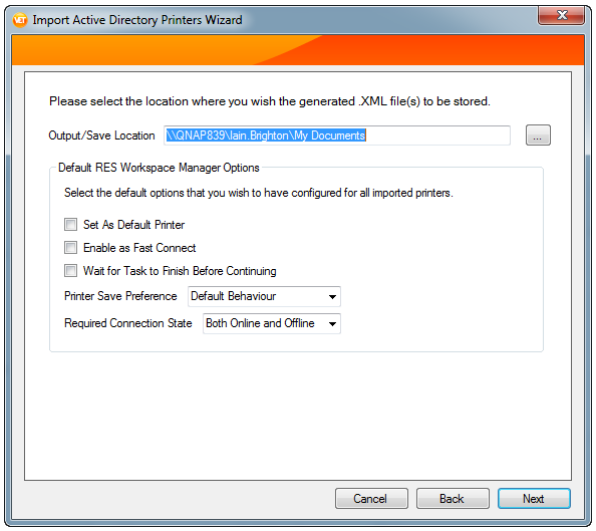
The ***Import Active Directory Printers Wizard*** will need to connect to Active Directory to locate all the published printer information. If you are connected to the domain from which you wish to import printers and logged on to the domain the ***Automatically detect Active Directory connection information*** option should suffice.

If you wish to import Active Directory information from another domain, are not logged on to the relevant domain or you are not performing the import from a domain joined computer, you will need to select the ***Manually specify Active Directory connection information*** option and complete the ***Domain Controller, Username*** and ***Password*** fields as necessary.

Once you have selected the applicable option, click ***Next*** to continue.

Copyright © 2008 – 2013 Virtual Engine Limited

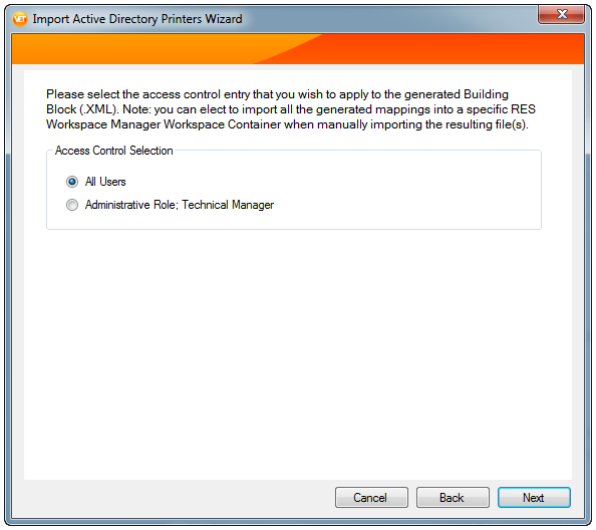
Figure 15 - Default Printer Options


Import Active Directory Printers Wizard
Please select the location where you wish the generated .XML file(s) to be stored.
Output/Save Location
\\QNAP839\Iain.Brighton\My Documents
Default RES Workspace Manager Options
Select the default options that you wish to have configured for all imported printers.
Set As Default Printer
Enable as Fast Connect
Wait for Task to Finish Before Continuing
Printer Save Preference
Default Behaviour
Required Connection State
Both Online and Offline
Cancel
Back
Next

If you wish to save the resulting .XML file in a location different to the default, enter the path in the ***Output/Save Location*** textbox or utilise the browse button to select an alternative directory.

For each printer that is created within RES Workspace Manager you will need to set the default options in the ***Default RES Workspace Manager Options*** section. Select the required options for ***Default Printer, Fast Connect, Synchronous/Asynchronous processing, Printer Preferences*** and ***Required Connection State***. The chosen defaults will be applied to all printers that are imported. When ready click the ***Next*** button.

Figure 16 - AD Printer Access Control

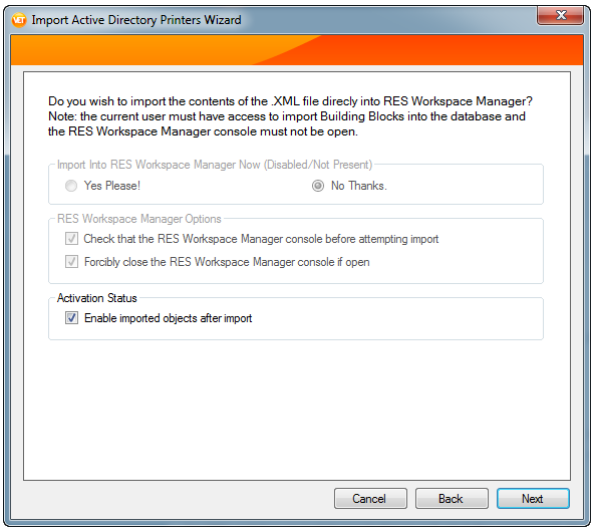

Import Active Directory Printers Wizard
Please select the access control entry that you wish to apply to the generated Building Block (.XML). Note: you can elect to import all the generated mappings into a specific RES Workspace Manager Workspace Container when manually importing the resulting file(s).
Access Control Selection
All Users
Administrative Role; Technical Manager
Cancel
Back
Next

If you wish all generated printer mapping to be available for all users, select the ***All Users*** option. To import the objects assigned to the ***RES Workspace Manager Technical Manager*** Administrative role (not initially available to users) then choose the ***Administrative Role; Technical Manager*** option.

Click ***Next*** to move onto the RES Workspace Manager import wizard.

Copyright © 2008 – 2013 Virtual Engine Limited

Figure 17 - AD Printer RES WM Import

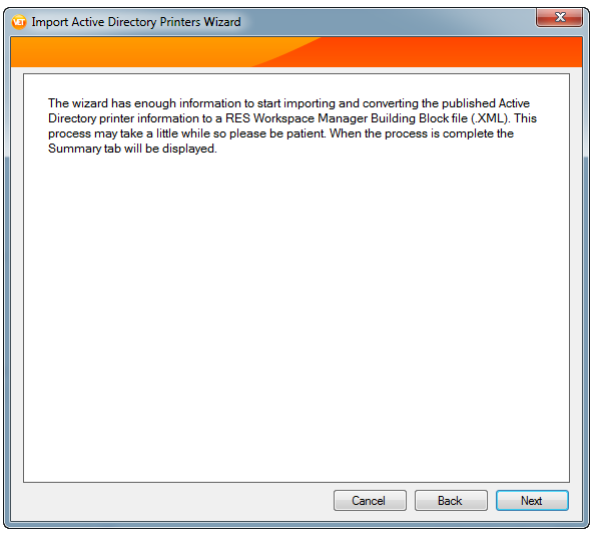

Import Active Directory Printers Wizard
Do you wish to import the contents of the .XML file direcly into RES Workspace Manager? Note: the current user must have access to import Building Blocks into the database and the RES Workspace Manager console must not be open.
Import Into RES Workspace Manager Now (Disabled/Not Present)
Yes Please!
No Thanks.
RES Workspace Manager Options
Check that the RES Workspace Manager console before attempting import
Forcibly close the RES Workspace Manager console if open
Activation Status
Enable imported objects after import
Cancel
Back
Next

If you wish to import the generated building blocks directly into the RES Workspace Manager console click the ***Yes Please!*** option. If the options are greyed out then the RES Workspace Manager console has not been detected or the integration has been disabled. For more information on the RES Workspace Manager integration and options please refer to the **Importing Building Blocks into RES Workspace Manager** section.

If you wish the resulting RES Workspace Manager objects to be automatically enabled after importing, ensure the ***Enable imported objects after import*** checkbox is selected. If you would like them disabled, ensure it is unchecked.

Click the ***Next*** button.

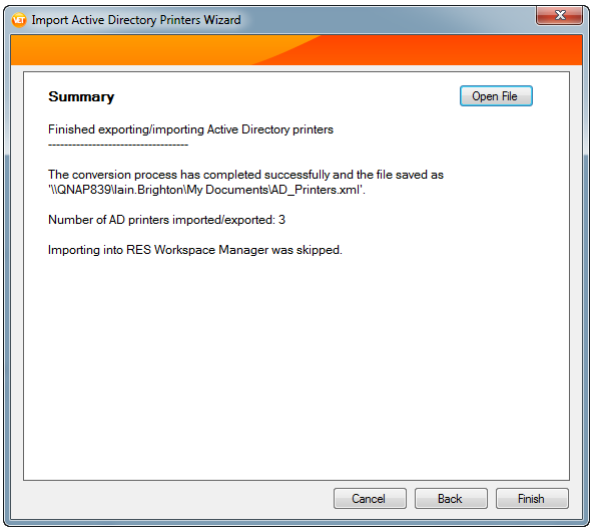
Figure 18 - AD Printers Import Ready


Import Active Directory Printers Wizard
The wizard has enough information to start importing and converting the published Active Directory printer information to a RES Workspace Manager Building Block file (.XML). This process may take a little while so please be patient. When the process is complete the Summary tab will be displayed.
Cancel
Back
Next

If all options have been completed and configured correctly, the wizard will inform you it's ready to perform the conversion and import (if selected). Click the ***Next*** button to start the process.

Copyright © 2008 – 2013 Virtual Engine Limited

Figure 19 - AD Printers Import Summary

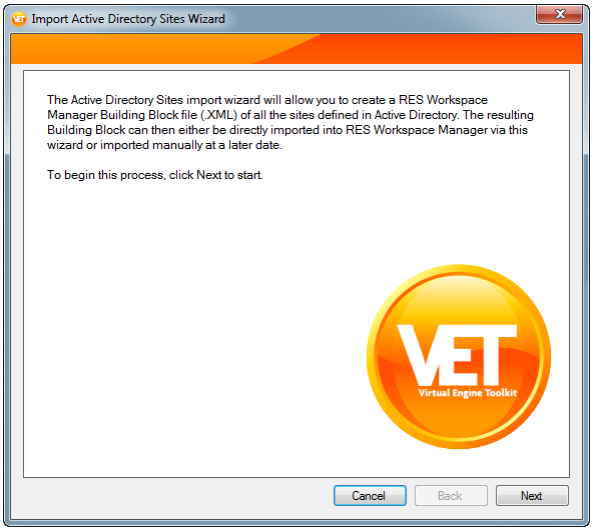

Import Active Directory Printers Wizard
Summary
Open File
Finished exporting/importing Active Directory printers
The conversion process has completed successfully and the file saved as '\\QNAP839\Iain.Brighton\My Documents\AD_Printers.xml'.
Number of AD printers imported/exported: 3
Importing into RES Workspace Manager was skipped.
Cancel
Back
Finish

Once the process is complete the summary screen will be displayed detailing the output file and location. If you wish to open the resulting .XML file, click the ***Open File*** button. To close the wizard click the ***Finish*** button.

Importing Active Directory Site Definitions

All configured Active Directory site definitions can be exported to a RES Workspace Manager building block file with the ***Import Active Directory Sites Wizard***. To launch the wizard click the ***Wizards > RES Workspace Manager > Import AD Sites*** menu option.

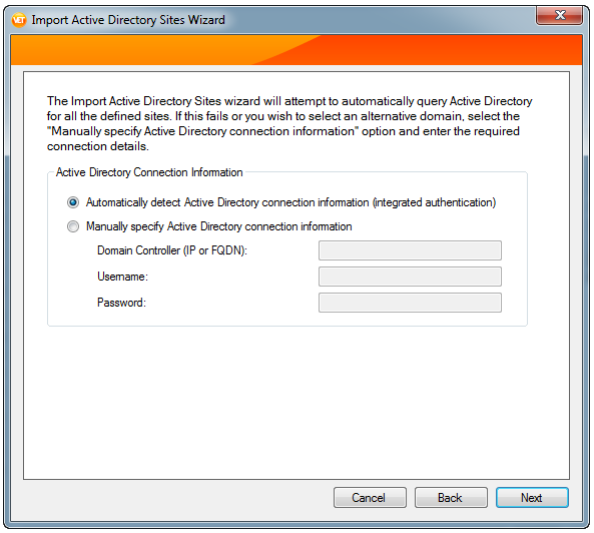
Figure 20 - Import AD Sitess Wizard


Import Active Directory Sites Wizard
The Active Directory Sites import wizard will allow you to create a RES Workspace Manager Building Block file (.XML) of all the sites defined in Active Directory. The resulting Building Block can then either be directly imported into RES Workspace Manager via this wizard or imported manually at a later date.
To begin this process, click Next to start.
VET
Virtual Engine Toolkit
Cancel
Back
Next

After reading the introductory information and you want to proceed, click the ***Next*** button.

Copyright © 2008 – 2013 Virtual Engine Limited

Figure 21 - AD Connection Information

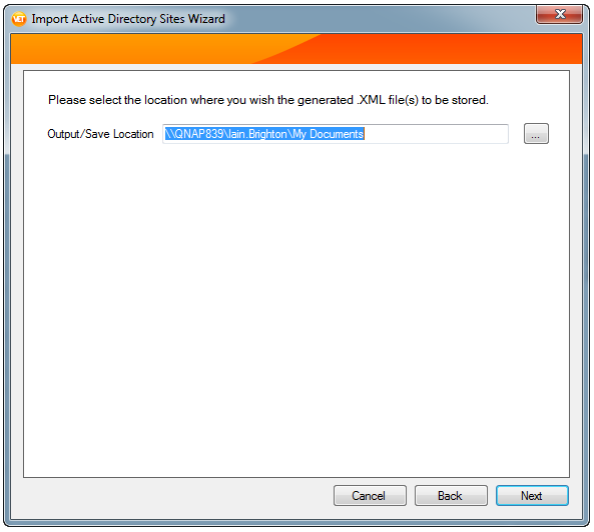

Import Active Directory Sites Wizard
The Import Active Directory Sites wizard will attempt to automatically query Active Directory for all the defined sites. If this fails or you wish to select an alternative domain, select the "Manually specify Active Directory connection information" option and enter the required connection details.
Active Directory Connection Information
Automatically detect Active Directory connection information (integrated authentication)
Manually specify Active Directory connection information
Domain Controller (IP or FQDN):
Username:
Password:
Cancel
Back
Next

The ***Import Active Directory Sites Wizard*** will need to connect to an Active Directory domain to locate all the defined site information. If you are connected to the domain from which you wish to import printers and logged on to the domain, the ***Automatically detect Active Directory connection information*** should suffice.

If you wish to import Active Directory information from another domain, are not logged on to the relevant domain or you are not performing the import from a domain joined computer you will need to select the ***Manually specify Active Directory connection information*** option and complete the ***Domain Controller, Username*** and ***Password*** fields as necessary.

Once you have selected the applicable option, click ***Next*** to continue.

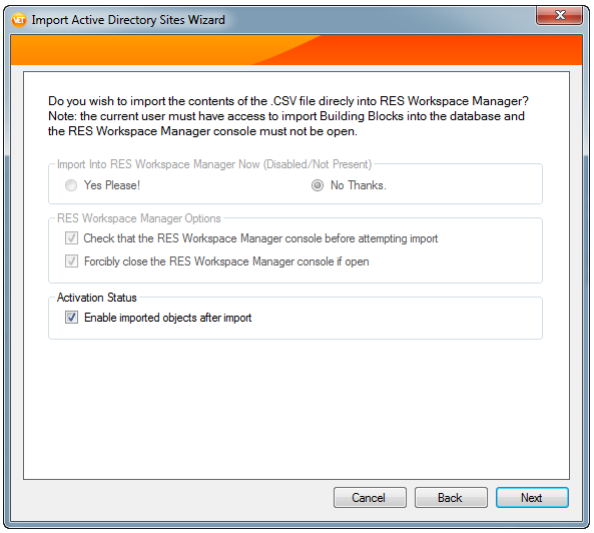
Figure 22 - Default Save Location



If you wish to save the resulting .XML file in a location that is different to the default, enter the path in the ***Output/Save Location*** textbox or utilise the browse button. When ready click the ***Next*** button.

Copyright © 2008 – 2013 Virtual Engine Limited

Figure 23 - AD Sites RES WM Import

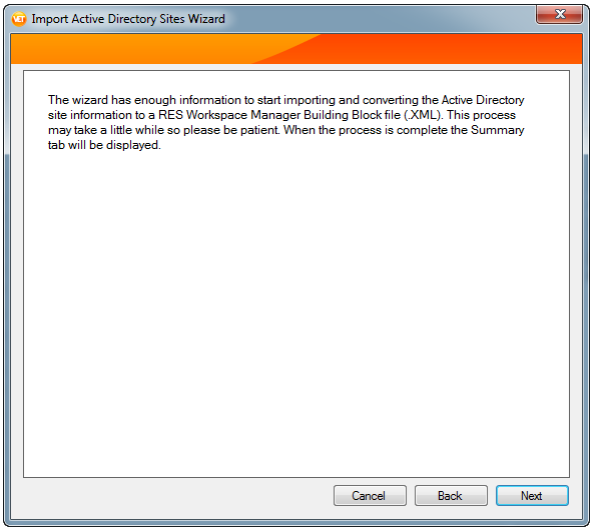

Import Active Directory Sites Wizard
Do you wish to import the contents of the .CSV file direcly into RES Workspace Manager? Note: the current user must have access to import Building Blocks into the database and the RES Workspace Manager console must not be open.
Import Into RES Workspace Manager Now (Disabled/Not Present)
Yes Please!
No Thanks.
RES Workspace Manager Options
Check that the RES Workspace Manager console before attempting import
Forcibly close the RES Workspace Manager console if open
Activation Status
Enable imported objects after import
Cancel
Back
Next

This wizard will ask if you wish to import the information directly into RES Workspace Manager console. If the options are unavailable then the RES Workspace Manager console has not been detected or the integration has been disabled. For more information on the RES Workspace Manager integration and options please refer to the **Importing Building Blocks into RES Workspace Manager** section.

If you wish the resulting RES Workspace Manager objects to be enabled after importing, ensure the ***Enable imported objects after import*** checkbox is selected. If you want them disabled, ensure it is unchecked.

Click the ***Next*** button.

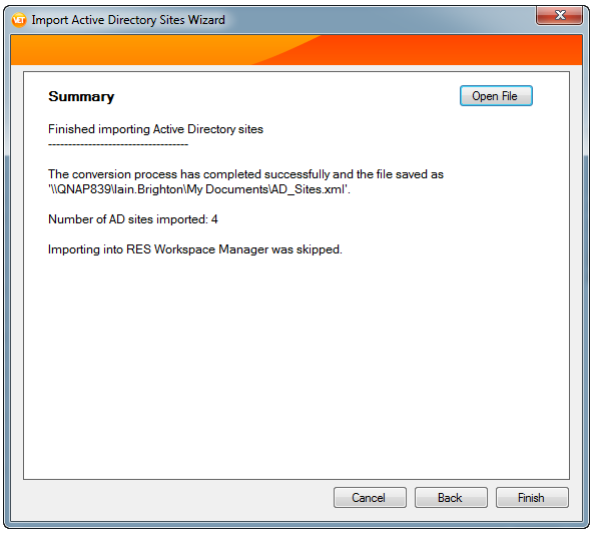
Figure 24 - AD Printers Import Ready


Import Active Directory Sites Wizard
The wizard has enough information to start importing and converting the Active Directory site information to a RES Workspace Manager Building Block file (.XML). This process may take a little while so please be patient. When the process is complete the Summary tab will be displayed.
Cancel
Back
Next

If all options have been completed and configured correctly, the wizard will inform you it's ready to perform the conversion and direct import (if selected). Click the ***Next*** button to start the process.

Copyright © 2008 – 2013 Virtual Engine Limited

Figure 25 - AD Sites Conversion Summary


Import Active Directory Sites Wizard
Summary
Open File
Finished importing Active Directory sites
The conversion process has completed successfully and the file saved as '\\QNAP839\Iain.Brighton\My Documents\AD_Sites.xml'.
Number of AD sites imported: 4
Importing into RES Workspace Manager was skipped.
Cancel
Back
Finish

Once the process is complete the summary screen will be displayed detailing the output file and location. If you wish to open the resulting .XML file, click the ***Open File*** button. To close the wizard click the ***Finish*** button.

Copyright © 2008 – 2013 Virtual Engine Limited

BBSpinner

The Building Block Spinner (or BBSpinner) is primarily used in large RES Workspace Manager environments where more than one database is utilised and different Active Directory domains and/or forests are present. This functionality can also be used by RES customers and partners to import preconfigured Building Blocks for Proof of Concept (PoC) or production deployments.

When Building Blocks are exported from a RES Workspace Manager database, all source Access Control entries are embedded within the resulting XML file(s). This is fine if the destination RES Workspace Manager database/users are authenticating against the same Active Directory.

However, if the Active Directory domain names are different then a manual update is required before the Building Block(s) are imported, typically via a manual "Find and Replace" function. All references to DOMAIN1\ need to be replaced with DOMAIN2\.

Note

There is also no inbuilt verification that the Access Control entries contained within a Building Block can be resolved once the import process is complete.

In addition, changes might be originating from both environments complicating things further. Take the following example:

- CompanyX has a testing and development environment that is completely segmented from the production network. The NetBIOS domain name of this environment is TEST.
- The live/production environment NetBIOS domain name is called LIVE.
- All controlled changes originate from the TEST domain and need to be implemented in the LIVE environment.
- File authorisation changes originate from the LIVE domain and need to be ported back into the TEST environment.
- Active Directory group names are consistent between each environment, although the domain names are different.

The BBSpinner solves this issue by taking all Building Block files (created in both environments) and creates two sets of XML files, one set that can be imported directly into each environment; one for TEST and one for LIVE.

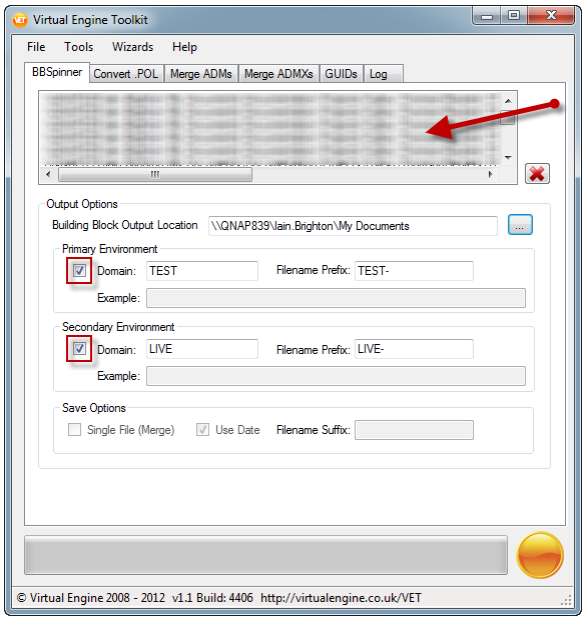
Copyright © 2008 – 2013 Virtual Engine Limited

Using BBSpinner

To use the BBSpinner complete the following steps:

1. Select the BBSpinner tab within the user interface.
2. Drag and drop the source Building Block file(s) into the top box on the BBSpinner tab (highlighted in Figure 26 - BBSpinner). **Note: Files can be removed from the list by highlighting them and clicking the button.**
3. Select the Building Block file output location by entering it in the "Building Block Output Location" text box or by selecting the button.
4. If you require the BBSpinner to create files for the Primary environment, ensure that you check the checkbox under the Primary Environment header (highlighted in Figure 26 - BBSpinner).
5. Enter a domain name in the "Primary Environment: Domain" text box. This should be the NetBIOS domain name, e.g. LIVE.
6. All files that are outputted by the BBSpinner for this domain will utilise the original filename but prefixed with what is specified in the "Primary Environment: Filename Prefix" textbox, i.e. "LIVE-". For example, if the source XML filename is "start_my_computer.xml" the BBSpinner will write the new XML file as "LIVE-start_my_computer.xml".
7. Repeat steps 3 – 5, but for the Secondary environment.
8. Once ready to create one or two sets of Building Blocks, click the orb in the bottom right of the VET interface (highlighted in Figure 26 - BBSpinner).

Figure 26 - BBSpinner



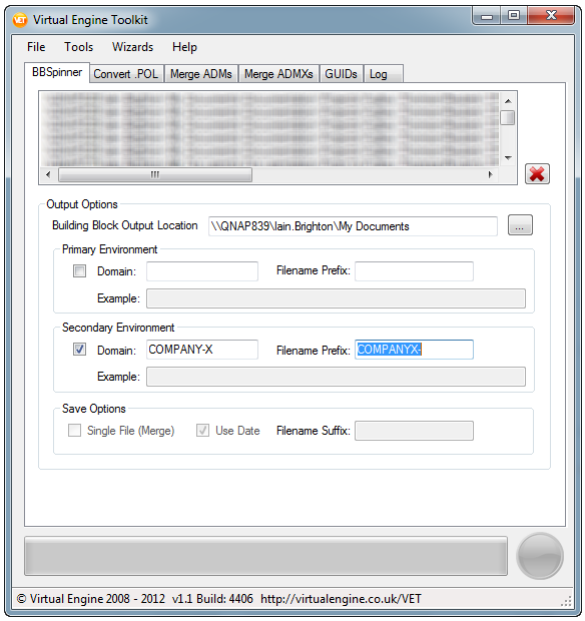
It is possible to only output one set of building blocks by only enabling either the primary or secondary environment. For example, consulting partners can configure all their proprietary Building Blocks with a development/test domain, e.g. TEST\. Using the following settings will enable easy deployment into CompanyX's environment with the COMPANY-X\ domain.

Copyright © 2008 – 2013 Virtual Engine Limited

Note

The Active Directory groups specified in access control entries within the Building Blocks will need to be present in the COMPANY-X domain.

Figure 27 – Quick Deploy using the BBSpinner



The BBSpinner will take all Building Blocks specified and replace all "TEST\" Access Control entries with "COMPANY-X\" and write them to the specified output directory, ready for importing directly into the customer's environment. Only the Secondary environment Building Blocks will be generated as the Primary (TEST) environment has not been enabled.

Copyright © 2008 – 2013 Virtual Engine Limited

Convert POLs

The ***Convert POLs*** tab provides a simple way to import an existing Group Policy Object into your User Environment Management tool of choice. A lot of background information on what can/can't be imported and the .POL file format can be found on the Virtual Engine web site in the following Virtual Engine posts:

- Migrating GPOs to RES PowerFuse (Part 1)
- Migrating GPOs to RES PowerFuse (Part 2)
- Migrating GPOs to RES PowerFuse (Part 3)
- Migrating GPOs to RES Workspace Manager (Part 4)

Note: Multiple Group Policy Objects can be converted using the Conversion Wizard.

Note

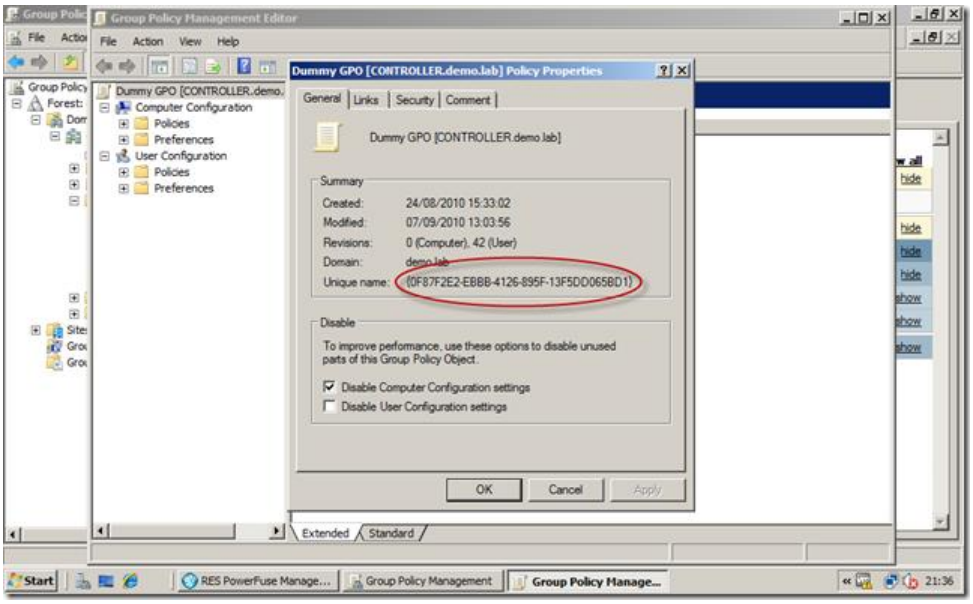
Only Group Policy Objects that the currently logged on user can read will be populated in the conversion wizard.

Running the Conversion WizardLocating Group Policy Object GUIDs

To begin converting an existing Group Policy object you have to know where the GPO is stored. To locate the relevant REGISTRY.POL file perform the following steps:

1. Open the Group Policy Management Console (GPMC).
2. Locate and edit the Group Policy Object that you wish to migrate.
3. Right-click the <GPO Name> in the navigation pane and select ***Properties*** from the resulting context menu.
4. The GPO's GUID will be displayed next to the ***Unique Name*** entry (see **Figure 28 - Locating a GPO GUID**).
5. Copy and/or write the GUID down as you will need it later!

Figure 28 - Locating a GPO GUID



Copyright © 2008 – 2013 Virtual Engine Limited

WARNING

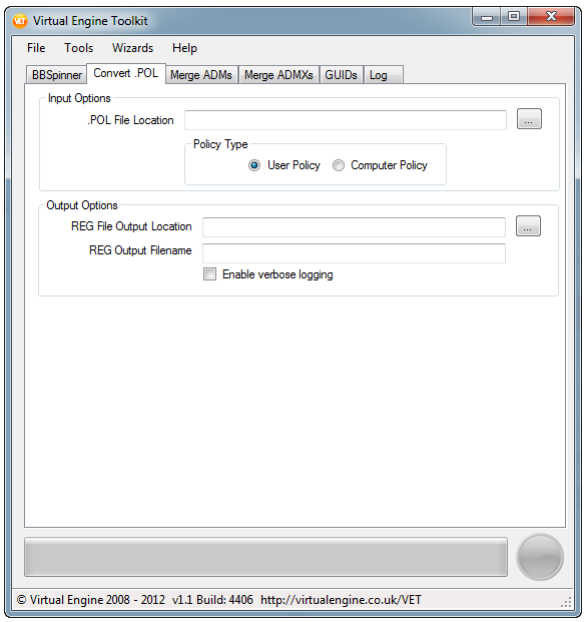
It is important to understand the REGISTRY.POL files contain no information on whether the settings contained within are applicable to HKLM or HKCU. Selecting the wrong .POL may lead to unexpected results!

Converting the REGISTRY.POL File

Now that GPO GUID has been located, the correct REGISTRY.POL file can be converted to a registry (.REG) file by performing the following actions:

1. Launch the Virtual Engine Toolkit and select the ***Convert POL*** tab.
2. Click the … next to the ***.POL File Location*** textbox.
3. Navigate to the \\<Domain FQDN>\SYSVOL\<Domain FQDN\Policies folder where <Domain FQDN> represents the FQDN of the Active Directory domain you wish to import the GPO from.
4. Select the directory that matches the Group Policy Object GUID referenced earlier.
5. Open the USER or MACHINE folder (this contains the 'User Configuration' or 'Computer Configuration' settings of the Group Policy Object).
6. Choose the REGISTRY.POL file.
7. Flag whether the ***Policy Type*** of the source .POL file is a machine or user policy by selecting either the ***User Policy*** or ***Computer Policy*** radio button. **Note: selecting the wrong policy type will lead to unexpected results!**
8. Select the output location to save the .REG file in the ***REG File Output Location*** text box.
9. Give the output .REG file a name in the ***REG Output Filename*** text box. **Note: the .REG file extension will be appended automatically.**
10. Once ready to create the .REG file, click the orb in the bottom right corner of the VET interface.

Figure 29 - Convert POLs



Importing GPOs Directly from Active Directory

Multiple Group Policy Objects can be imported from Active Directory via the ***Wizards > Convert Group Policy Objects*** menu in the VET menu bar. VET will attempt to automatically detect the required Active Directory domain information from the underlying Operating System.

Requirements

The ability to import Group Policy Objects requires a connection to a domain controller via LDAP and CIFS. The LDAP connection is required to query Active Directory for various GPO settings and security permissions.

For the auto detection to work successfully, it is required that the user is logged on with a domain account in the Active Directory domain the Group Policy Objects will be imported from.

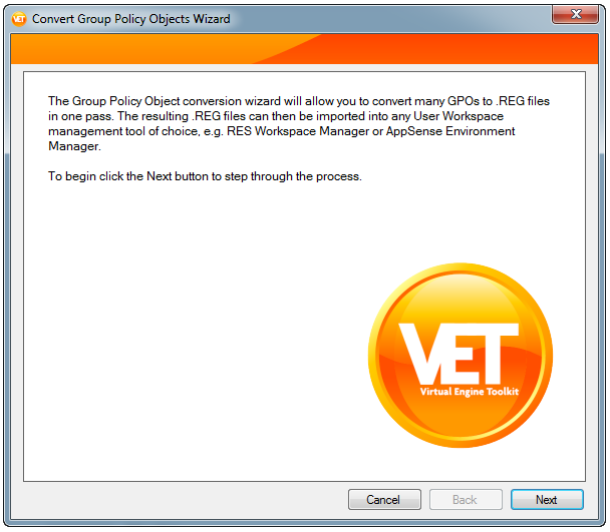
Note

Only Group Policy Objects that the currently logged on user can read will be populated in the conversion wizard.

Running the Conversion Wizard

The ***Convert GPOs*** wizard can be started from the ***Wizards > Convert Group Policy Objects*** menu. The wizard can be aborted at any time by clicking the ***Cancel*** button.

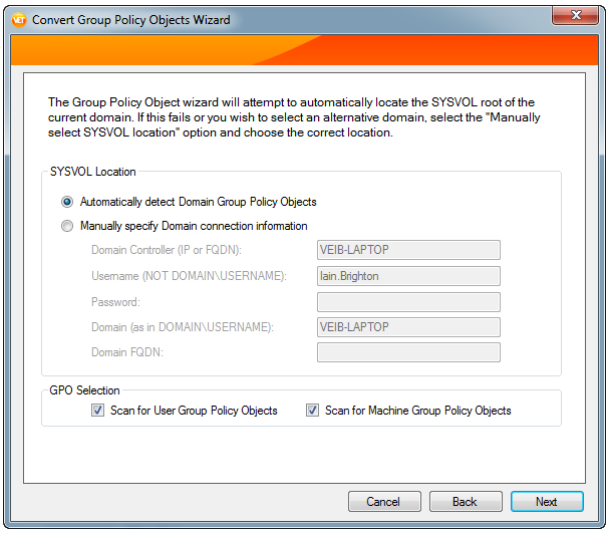
Figure 30 - Convert GPOs Wizard


Convert Group Policy Objects Wizard
The Group Policy Object conversion wizard will allow you to convert many GPOs to .REG files in one pass. The resulting .REG files can then be imported into any User Workspace management tool of choice, e.g. RES Workspace Manager or AppSense Environment Manager.
To begin click the Next button to step through the process.
VET
Virtual Engine Toolkit
Cancel
Back
Next

Read the *Welcome* information and click ***Next***. The wizard will attempt to automatically connect to Active Directory using the logged on user credentials.

Copyright © 2008 – 2013 Virtual Engine Limited

Figure 31 - Active Directory Automatic Detection


Convert Group Policy Objects Wizard
The Group Policy Object wizard will attempt to automatically locate the SYSVOL root of the current domain. If this fails or you wish to select an alternative domain, select the "Manually select SYSVOL location" option and choose the correct location.
SYSVOL Location
Automatically detect Domain Group Policy Objects
Manually specify Domain connection information
Domain Controller (IP or FQDN):
VEIB-LAPTOP
Username (NOT DOMAIN\USERNAME):
Iain.Brighton
Password:
Domain (as in DOMAIN\USERNAME):
VEIB-LAPTOP
Domain FQDN:
GPO Selection
Scan for User Group Policy Objects
Scan for Machine Group Policy Objects
Cancel
Back
Next

By default the Convert GPOs wizard will attempt to enumerate the Administrative Templates section of User Group Policy Object configuration containers as these are the only policies supported by RES Workspace Manager. If you wish to only evaluate one or the other, deselect either the ***Scan for User Group Policy Objects*** or ***Scan for Machine Group Policy Objects*** checkboxes as necessary.

Note

Computer Group Policy Objects can only be converted to registry files (.REG). If you choose to convert these policies, they will not be included in any RES Workspace Manager building block file(s).

After completing the required connection state information, click ***Next*** to proceed. At this point, VET will attempt to connect to both the Active Directory and SYSVOL volume to enumerate all the available Group Policy Objects.

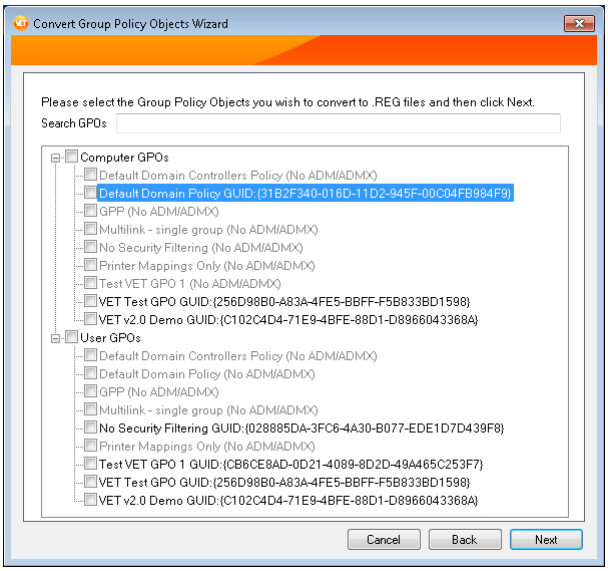
Note

Group Policy objects that do not contain any Administrative Templates (ADM or ADMX) settings will be greyed out and will not be converted.

Once the process is complete, the wizard will display all the discovered GPOs with their display names and GUIDs.

Copyright © 2008 – 2013 Virtual Engine Limited

Figure 32 - Select GPOs for Conversion

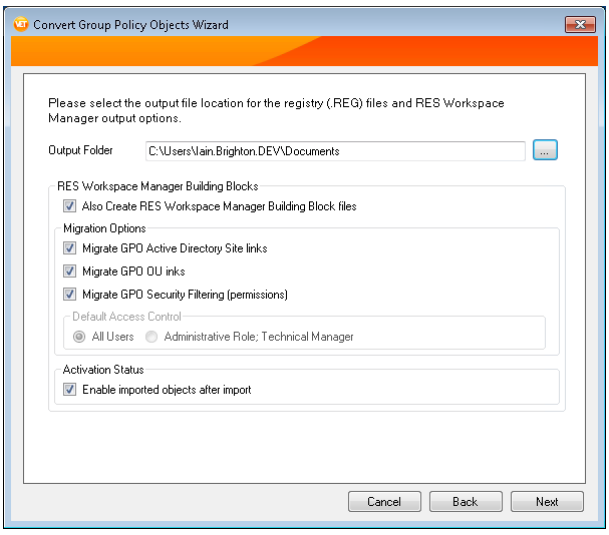

Convert Group Policy Objects Wizard
Please select the Group Policy Objects you wish to convert to .REG files and then click Next.
Search GPOs
Computer GPOs
Default Domain Controllers Policy (No ADM/ADMX)
Default Domain Policy GUID:{31B2F340-016D-11D2-945F-00C04FB984F9}
GPP (No ADM/ADMX)
Multilink - single group (No ADM/ADMX)
No Security Filtering (No ADM/ADMX)
Printer Mappings Only (No ADM/ADMX)
Test VET GPO 1 (No ADM/ADMX)
VET Test GPO GUID:{256D98B0-A83A-4FE5-BBFF-F5B833BD1598}
VET v2.0 Demo GUID:{C102C4D4-71E9-4BFE-88D1-D8966043368A}
User GPOs
Default Domain Controllers Policy (No ADM/ADMX)
Default Domain Policy (No ADM/ADMX)
GPP (No ADM/ADMX)
Multilink - single group (No ADM/ADMX)
No Security Filtering GUID:{028885DA-3FC6-4A30-B077-EDE1D7D439F8}
Printer Mappings Only (No ADM/ADMX)
Test VET GPO 1 GUID:{CB6CE8AD-0D21-4089-8D2D-49A465C253F7}
VET Test GPO GUID:{256D98B0-A83A-4FE5-BBFF-F5B833BD1598}
VET v2.0 Demo GUID:{C102C4D4-71E9-4BFE-88D1-D8966043368A}
Cancel
Back
Next

The ***Select GPOs*** screen will display all the available GPOs that either have user and/or computer configuration options set. Therefore, if you have a GPO with both user and computer options configured, it will appear beneath both the ***User GPOs*** and ***Computer GPOs*** nodes in the tree view.

To narrow your search down when a large amount of results are returned, use the ***Search GPOs*** field to start the keyword pattern matching facility. The results will be highlighted as you type, assisting with finding and selecting numerous Group Policies.

Place a check in the checkbox next to all the Group Policy Objects that you wish to convert to .REG files. Once complete, click the ***Next*** button to display the output/save options.

Figure 33 - Covert GPOs Output Options


Convert Group Policy Objects Wizard
Please select the output file location for the registry (.REG) files and RES Workspace Manager output options.
Output Folder
C:\Users\Iain.Brighton.DEV\Documents
RES Workspace Manager Building Blocks
Also Create RES Workspace Manager Building Block files
Migration Options
Migrate GPO Active Directory Site links
Migrate GPO OU inks
Migrate GPO Security Filtering (permissions)
Default Access Control
All Users
Administrative Role; Technical Manager
Activation Status
Enable imported objects after import
Cancel
Back
Next

Select the folder in which you wish the resulting registry files to be saved in the ***Output Folder*** text box.

Copyright © 2008 – 2013 Virtual Engine Limited

If you require additional RES Workspace Manager building block (.XML) files to be created, ensure the ***Also Create RES Workspace Manager Building Block files*** option is checked. The resulting .XML files can be imported into the RES Workspace Manager console.

VET can now migrate Group Policy Object organisational unit and active directory site links as well as security filtering ("Apply Group Policy" Active Directory extended rights) applied to the GPO. If you wish to migrate leave the default options selected. If you don't wish to migrate the links, deselect the appropriate option.

If you choose not to migrate the Group Policy Object security filtering you will need to choose the default access control applied to the resulting RES Workspace Manager objects.

Note

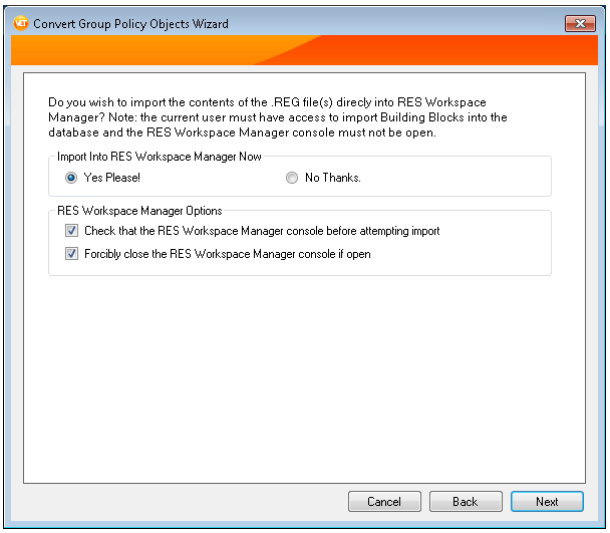
The generated building block file(s) refer to the created registry files. If manually importing the .XML files, the related .REG files are also required (and must be located in the same folder) during import.

Note

For more detailed information on how Group Policy Object links and security filtering is migrated, please refer to Appendix A.

Click ***Next*** to move onto the RES Workspace Manager import options screen.

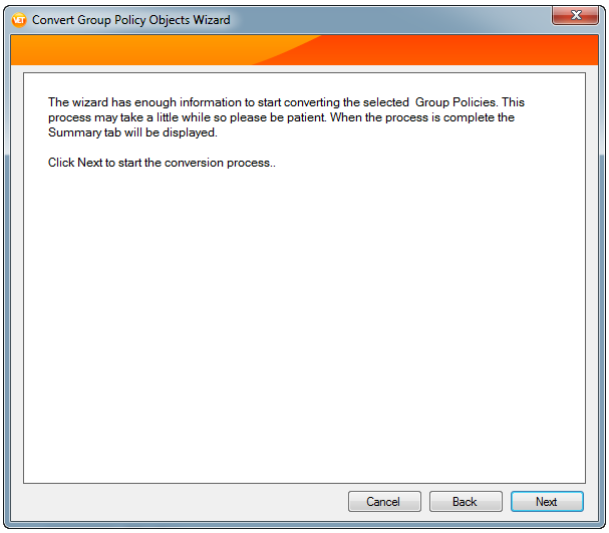
Figure 34 - RES WM Import Options


Convert Group Policy Objects Wizard
Do you wish to import the contents of the .REG file(s) direcly into RES Workspace Manager? Note: the current user must have access to import Building Blocks into the database and the RES Workspace Manager console must not be open.
Import Into RES Workspace Manager Now
Yes Please!
No Thanks.
RES Workspace Manager Options
Check that the RES Workspace Manager console before attempting import
Forcibly close the RES Workspace Manager console if open
Cancel
Back
Next

When you have correctly configured the RES Workspace Manager import options as required, click ***Next*** to move on to the next screen.

Copyright © 2008 – 2013 Virtual Engine Limited

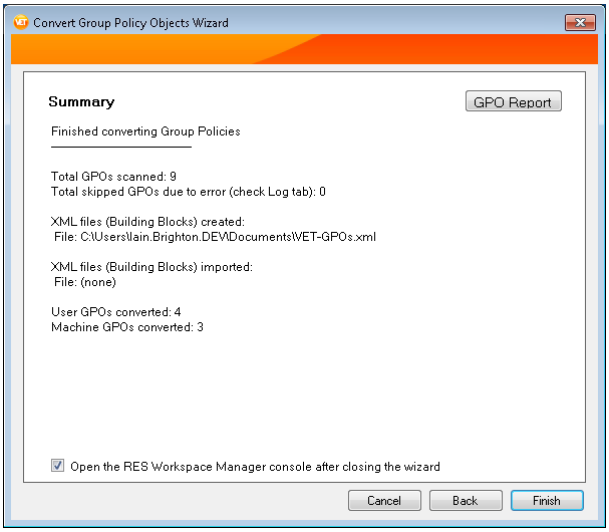
Figure 35 - Convert GPOs Ready..


Convert Group Policy Objects Wizard
The wizard has enough information to start converting the selected Group Policies. This process may take a little while so please be patient. When the process is complete the Summary tab will be displayed.
Click Next to start the conversion process..
Cancel
Back
Next

The wizard should have all the information required to complete the conversion process. When ready click the ***Next*** button to start converting Group Policy Objects.

Once the process is complete, the wizard will display summary information as shown below. Click the ***Finish*** button to close the wizard. The registry files will be saved in the 'TYPE – GPO Display Name.reg' format in the specified output folder. For example, a machine based GPO with a display name of 'Default Computer Settings' will be named ***MACHINE default-computer-settings.reg***.

Figure 36 - Convert GPOs Summary

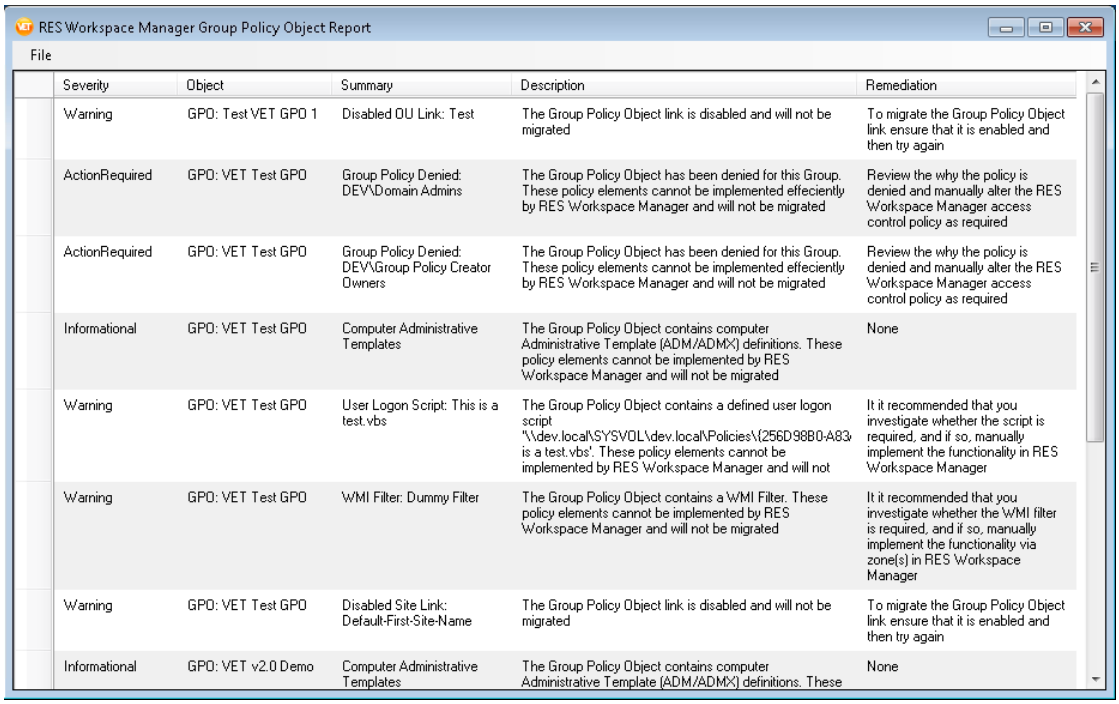


Since VET v1.2, only a single RES Workspace Manager building block file will be created for all converted Group Policies (one registry file per GPO is still created). The ***VET-GPOs.xml*** file is located in the specified output directory along with the registry (.REG) files.

A new Group Policy Object report option is available that warns of any settings within the converted GPOs that cannot be implemented efficiently within RES Workspace Manager. Examples include, "Apply Group Policy" denied access control entries, disabled links and the presence of any logon/logoff scripts etc. To view the report, click the ***GPO Report*** button.

Copyright © 2008 – 2013 Virtual Engine Limited

Figure 37 - GPO Summary Report



Severity	Object	Summary	Description	Remediation
Warning	GPO: Test VET GPO 1	Disabled OU Link: Test	The Group Policy Object link is disabled and will not be migrated	To migrate the Group Policy Object link ensure that it is enabled and then try again
ActionRequired	GPO: VET Test GPO	Group Policy Denied: DEV\Domain Admins	The Group Policy Object has been denied for this Group. These policy elements cannot be implemented effeciently by RES Workspace Manager and will not be migrated	Review the why the policy is denied and manually alter the RES Workspace Manager access control policy as required
ActionRequired	GPO: VET Test GPO	Group Policy Denied: DEV\Group Policy Creator Owners	The Group Policy Object has been denied for this Group. These policy elements cannot be implemented effeciently by RES Workspace Manager and will not be migrated	Review the why the policy is denied and manually alter the RES Workspace Manager access control policy as required
Informational	GPO: VET Test GPO	Computer Administrative Templates	The Group Policy Object contains computer Administrative Template (ADM/ADMX) definitions. These policy elements cannot be implemented by RES Workspace Manager and will not be migrated	None
Warning	GPO: VET Test GPO	User Logon Script: This is a test.vbs	The Group Policy Object contains a defined user logon script '\\dev.local\SYSVOL\dev.local\Policies\{256D98B0-A83 is a test.vbs'. These policy elements cannot be implemented by RES Workspace Manager and will not	It it recommended that you investigate whether the script is required, and if so, manually implement the functionality in RES Workspace Manager
Warning	GPO: VET Test GPO	WMI Filter: Dummy Filter	The Group Policy Object contains a WMI Filter. These policy elements cannot be implemented by RES Workspace Manager and will not be migrated	It it recommended that you investigate whether the WMI filter is required, and if so, manually implement the functionality via zone(s) in RES Workspace Manager
Warning	GPO: VET Test GPO	Disabled Site Link: Default-First-Site-Name	The Group Policy Object link is disabled and will not be migrated	To migrate the Group Policy Object link ensure that it is enabled and then try again
Informational	GPO: VET v2.0 Demo	Computer Administrative Templates	The Group Policy Object contains computer Administrative Template (ADM/ADMX) definitions. These	None

Copyright © 2008 – 2013 Virtual Engine Limited

Merge ADMs and Merge ADMXs

The .ADM and .ADMX merging functionality enables administrators to consolidate multiple GPO template files into a single entity for management within the User Environment Management tool of choice. Without this, multiple User Registry Policies need to be created within the console as each policy can typically only be based on an individual .ADM or .ADMX file.

Note

It is not possible to merge .ADM file(s) with .ADMX file(s). Only files of the same type can be merged together.

ADMX File Format

The .ADMX file format (Windows Vista and Windows 2008 onwards) for Group Policy templates is different from the legacy (Windows 2000 to Windows 2003) .ADM format. The primary difference is that the language of the .ADM file is contained within the file itself. Therefore, the en-US version of XYZ.ADM is completely different to the fr-FR version of XYZ.ADM. In contrast, the .ADMX file contains all the logic within a policy .ADMX template, but it must be accompanied by a corresponding .ADML file which contains the language abstraction, e.g. English or French.

When using the Virtual Engine Toolkit to merge .ADMXs, VET will search the same directory as the source .ADMX file for a corresponding .ADML file. If one is not found, it will search all sub directories and use the first match found. If no .ADML file is found an error will be displayed and the process aborted.

Tip

Virtual Engine provides many preconfigured merged .ADMX/L files for download on the web site: http://virtualengine.co.uk/downloads.

Merging ADMs/ADMXs

To use the GPO template merge facility, complete the following steps:

1. Select either the ***Merge ADMs*** or ***Merge ADMXs*** tab as required within the UI.
2. Drag and drop the ADMs (or ADMXs) you require to be merged into the top box on the relevant tab (see **Figure 38**).
3. Select the .ADM/.ADMX file save path by entering it in the ***ADM(X) File Output Location*** text box or by selecting the … button.
4. Enter the output file name (without the .ADM/.ADMX extension as this will be automatically appended) in the ***ADM(X) Output Filename*** text box.
5. Click the orb in the bottom right corner of the VET interface to create the merged .ADM (or .ADMX and .ADML) file.
6. Open the RES Workspace Manager console and create a new User Registry Policy and when prompted locate the file(s) created in Step 5.

Copyright © 2008 – 2013 Virtual Engine Limited

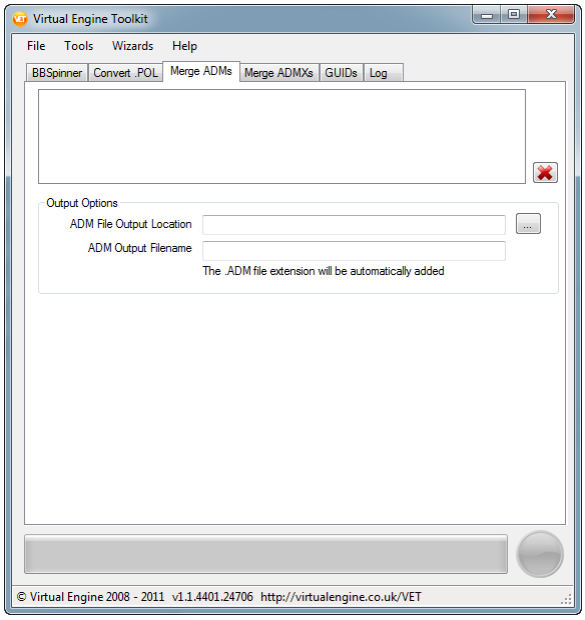
Note

If merging .ADMX files, ensure that the .ADML file is available when importing into the RES Workspace Manager console!

Tip

It is possible to use .ADMX/L files with AppSense Environment Manager and/or RES Workspace Manager when running a Windows 2000/2003 level domain.

Figure 38 - Merge ADM/ADMX



GUIDs Locator

RES Workspace Manager allows administrators to configure various elements of user's workspace or environment. Some of these tasks can also configured to only run once thus speeding up log in times as objects are not reapplied at every log in. The RES Workspace Manager console enables an administrator to clear the history for all users to force a given object to be reapplied.

In certain circumstances it is desirable to force a task to re-run only for a given user, but not everyone. In this instance an administrator must delete the relevant .ONCE file from the user's ***\PWRMENU*** (Pre RES Workspace Manager 2012) or **\Personal Settings** (RES Workspace Manager 2012) directory. Unfortunately, this file is named with a GUID that is not readily exposed in the RES Workspace Manager console.

.ONCE File Locations

To add a certain amount of confusion, the location of the .ONCE files depends on whether the configuration task is configured on a per user or computer basis. Files for per computer based tasks

Copyright © 2008 – 2013 Virtual Engine Limited

live within the RES Workspace Manager program directory and per user files are located within a user's ***PWRMENU*** or **Personal Settings** folder.

The following table details where each .(Run)Once file exists for each option available within the RES Workspace Manager console:

Type	File Location
Per User	<RESWM_UserSettings>\UserPref\<GUID>.ONCE
Per Computer	%RESPFDIR%\Data\DBCache\Objects\<GUID>.ONCE
Per Computer, Per User	%RESPFDIR%\Data\DBCache\Objects\<DOMAIN>_<USER>_<GUID>.ONCE

Retrieving RunOnce GUIDs

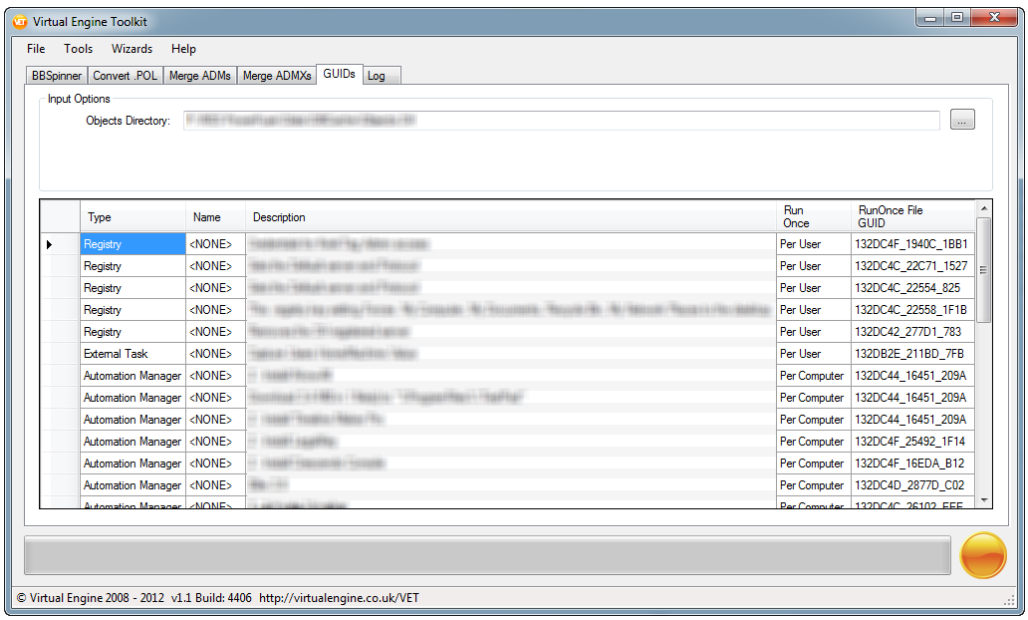
To find all the GUIDs for RunOnce tasks you can perform any of the following:

- Query each .XML file within %RESPFDIR%\DATA\DBCACHE\OBJECTS directory of a RES Workspace Manager agent installation;
- Export the object in question to a Building Block, open the .XML file and find the RunOnce GUID;
- Use the Virtual Engine Toolkit!

To start simply follow these steps:

1. Select the ***GUIDs*** tab within the VET window.
2. If RES Workspace Manager is detected on the local machine the ***Objects Directory*** location will automatically be completed. If this is not automatically completed browse to the ***Objects*** directory on a machine with RES Workspace Manager agent installed. **Note: this location is normally either %ProgramFiles%\RES PowerFuse\Data\DBCache\Objects or %ProgramFiles%\RES Software\Workspace Manager\Data\DBCache\Objects.**
3. Click the VET orb to enumerate all the RunOnce GUIDs as shown below.
4. You can use the discovered GUID to remove the relevant .ONCE file.

Figure 39 - RES Workspace Manager RunOnce GUIDs



Profile Update Utility

The VET Profile Update Utility (PuU) is a separate tool for updating and managing Windows Mandatory profiles. PuU solves one problem with mandatory profiles very well; updating them! In essence PuU allows an Administrator to select one or more existing user profile registry hives (NTUSER.DAT or NTUSER.MAN files) and inject registry settings into them.

The manual process for updating a mandatory profile is covered in the Virtual Engine Updating Mandatory Profiles blog post; http://virtualengine.co.uk/2011/updating-mandatory-profiles. Simplifying this example process with the Profile Update Utility only requires the administrator to just select the source Mandatory profile, select the ***Merge*** ActiveSetup button and click the ***Update*** button. DONE!

PuU allows any .REG file that contains HKEY_CURRENT_USER settings to be merged into one or more Mandatory profiles, in a single operation.

Note

As this utility requires additional Operating System privileges it is supplied as a separate application and shortcut. If running PuU on Windows Vista or later with UAC enabled, you will be prompted to run the executable with Administrator rights.

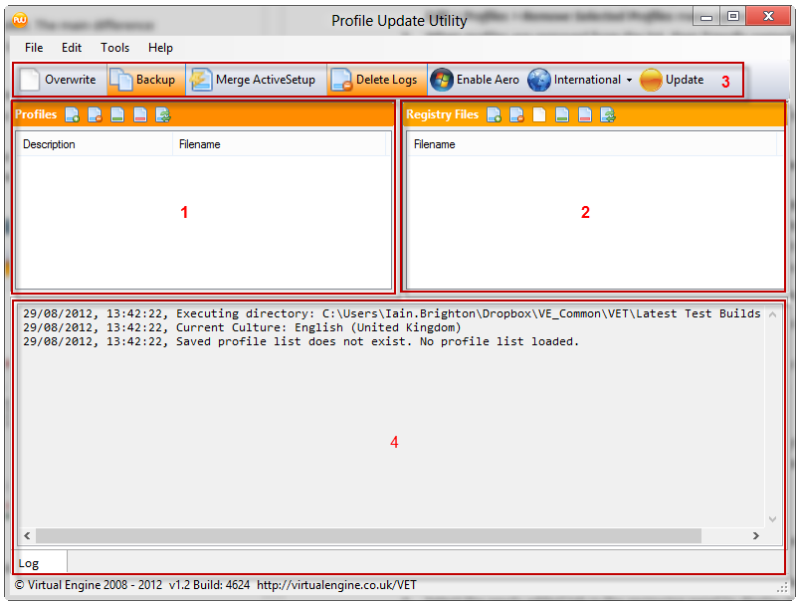
Copyright © 2008 – 2013 Virtual Engine Limited

The PuU Interface

The interface for PuU is very similar to that of the main Virtual Engine Toolkit. The main difference between VET and PuU is that drag and drop operations do not work with UAC enabled. This is a Windows security feature and not a restriction of PuU itself.

1. The left hand panel contains all the mandatory profiles that you may wish to update.
2. The registry files that you wish to merge into selected profiles are loaded into the right-hand panel.
3. The various backup modes and update options are selected in the top toolbar.
4. Logging information and registry files are loaded in the bottom reviewing panel.

Figure 40 - The PUU Interface



Adding/Removing Profiles

Before any profiles can be updated, they need to be loaded into the console. To add the user registry hives (.DAT or .MAN files) perform the following steps:

1. Either click the ***Add a mandatory profile to the profile list*** toolbar button or select the ***Edit > Profiles > Add Profiles*** menu option.
2. In the ***Open*** file window, select the target user registry hives (either a .MAN or .DAT files).
3. Click the ***Open*** button and the profile(s) will be loaded into the profile list.
4. Each profile can be given a description or friendly name as required. This helps identify different user profiles as they're typically all called NTUSER.DAT or NTUSER.MAN!
5. When a profile is first added, its description/friendly name is set to ***<None>.***
6. To give the profile a friendly name, click the ***<None>*** placeholder in the Description column and enter a friendly or descriptive name.
7. When the PuU interface is closed the loaded profile list and descriptions are saved.

If you wish to remove user profiles from the console, perform the following steps:

1. Select which profiles you wish to remove by checking the box next to all the profiles you wish to remove. **Note: Ensure any profiles you don't want to remove are unchecked.**

Copyright © 2008 – 2013 Virtual Engine Limited

2. Click either the ***Remove selected profiles from the profile list*** toolbar button or select the ***Edit*** > ***Profiles*** > ***Remove Selected Profiles*** menu option.
3. When profiles are removed from the list, their friendly name/description is not remembered and will be reset to ***<None>*** if re-added.

Adding/Removing Registry Files

Before registry files can be merged into user registry hives, they need to be loaded into the console. To add registry (.REG) files perform the following steps:

1. Either click the ***Add HKEY_CURRENT_USER registry files to the list*** toolbar button or select the ***Edit*** > ***Registry*** > ***Add Registry File(s)*** menu option.
2. In the ***Open*** file window, select the target user registry files (.REG files).
3. Click the ***Open*** button and the registry file(s) will be loaded into the registry list.
4. When the PuU interface is closed the loaded registry list is not remembered.
5. If the ***Merge ActiveSetup*** option is selected these registry files are automatically loaded.

If you wish to remove registry files from the console, perform the following steps:

1. Select which registry files you wish to remove by checking the box next to all the registry entries you wish to remove.
2. Click either the ***Remove selected registry from the list*** toolbar button or select the ***Edit*** > ***Registry Files*** > ***Remove Selected Registry Files*** menu option.

Ad-hoc Editing of Registry Files

It is possible to make ad-hoc changes to registry files prior to merging their contents into the selected user registry hives. To be able to make changes or view the contents of the .REG files, they first need to be mounted in the reviewing panel.

To mount a .REG file perform the following actions:

1. Right-click the registry file in the registry list that you wish to view and/or edit.
2. Select the ***Mount registry file*** option from the pop-up menu.
3. The registry file will be mounted in a new tab in the viewing panel.
4. Select the newly added tab in the reviewing panel to display its contents.
5. Make any changes required prior to merging. For example, the ActiveSetup registry keys can be reviewed and any user specific personalisation removed without having to edit the .REG file in an external editor.
6. Mounted registry files that have been changed but not saved are marked with an asterisk in the tab name.

If you wish to dismount a registry file from the reviewing panel, perform the following steps:

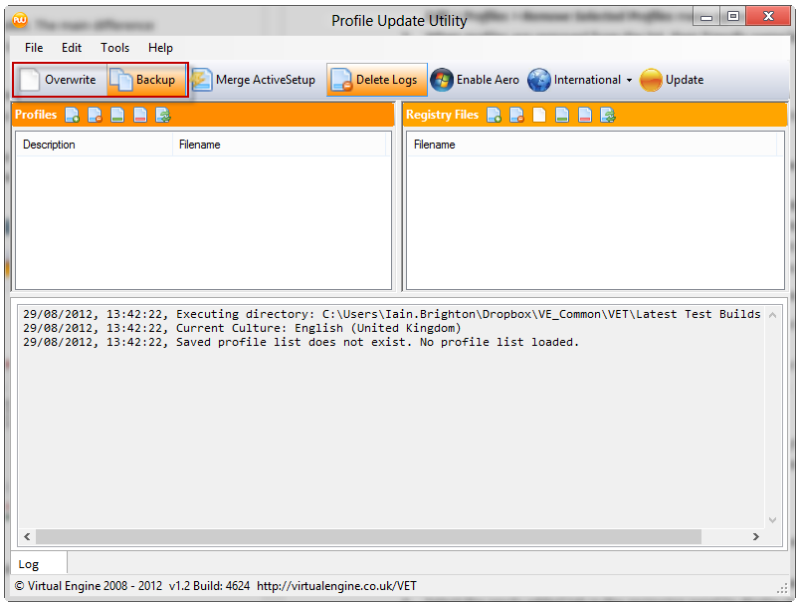
1. Right-click the mounted registry file in the registry list that you wish close or remove.
2. Select the ***Dismount registry file*** option from the pop-up menu.
3. If the mounted registry file has been changed, you will be prompted if you wish the alterations to be saved.
4. If you wish to save changes, select the ***Yes*** button from the ***Save Changes?*** window. If you wish to discard any changes, click the ***No*** button instead.

Copyright © 2008 – 2013 Virtual Engine Limited

Backup Options

The Profile Update Utility provides both an overwrite and a backup option when updating user registry hives (Profiles). These options are presented on the toolbar.

Figure 41 – PuU Backup Options



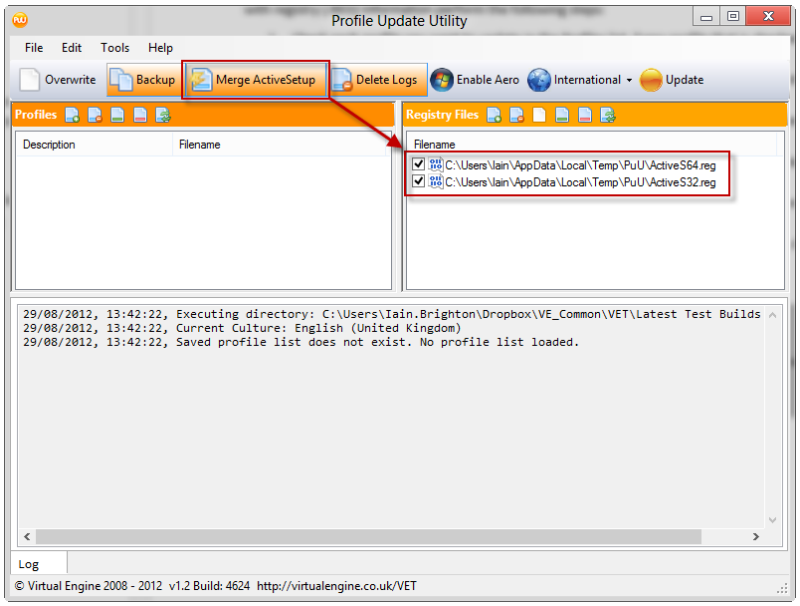
If the ***Overwrite*** option is selected, then all registry files will be merged into the selected profiles without any form of backup. The ***Backup*** option will copy the source profile to a .BAK file prior to making changes to the source profiles.

Windows ActiveSetup keys

If the ***Merge ActiveSetup*** keys option is enabled, then the Windows ActiveSetup keys from the local user are loaded into the ***Registry Files*** panel. If the console is running on 64-bit (x64) Operating System then two registry files will be loaded , i.e. the HLCU\Software\Wow6432Node\Microsoft\ActiveSetup locations as shown below.

Copyright © 2008 – 2013 Virtual Engine Limited

Figure 42 – PuU Merge ActiveSetup Keys



If you need to make changes to or review the ActiveSetup keys registry files, please refer to **Ad-hoc Editing of Registry Files**.

Deleting Profile Update Logs

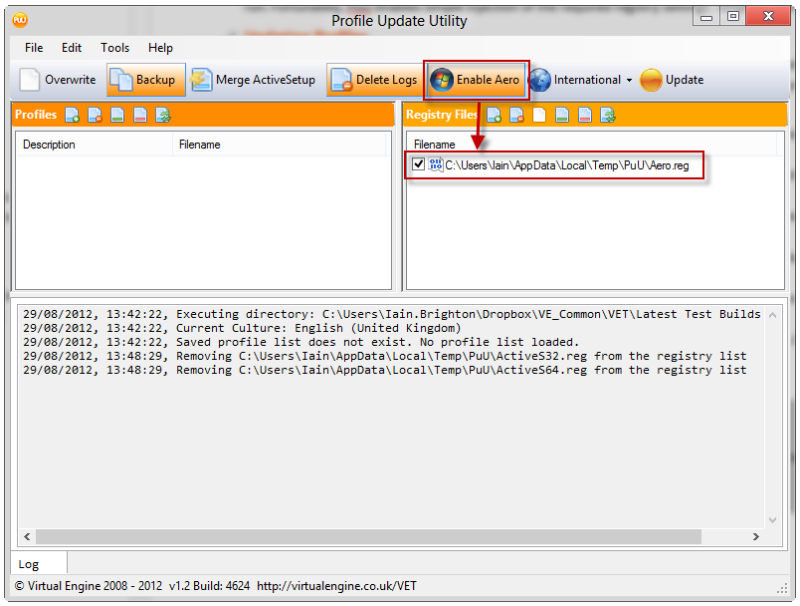
By default when user registry hives are mounted into the registry and updated, Windows will create various logging files. The Profile Update Utility can remove these log files if required. To enable this functionality ensure that the ***Delete Logs*** button is selected in the toolbar before updating the selected profiles.

Enabling Windows Aero Themes

Windows Aero themes are not necessarily enabled with Mandatory profiles if Active Setup does not run. Fortunately, PuU enables simple injection of the required registry settings. Simply click the ***Enable Aero*** button to load the required Windows Aero registry values into the ***Registry Files*** panel.

Copyright © 2008 – 2013 Virtual Engine Limited

Figure 43 - PuU Windows Aero Theme



WARNING

The Windows Aero theme is only supported on Version 2 Windows profiles (Windows Vista and later). PuU has no way of determining whether the target profiles are Version 1 or Version 2. Injecting the Windows Aero theme registry keys into a Version 1 profile will lead to unexpected results.

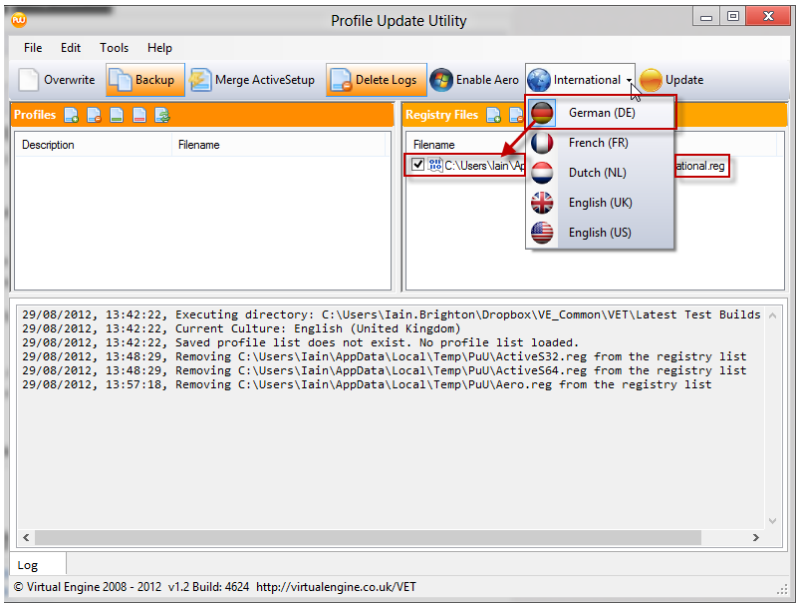
International and Regional Options

Setting the correct regional and international options within a Mandatory profile is not difficult once the require registry settings are known. To expedite this process PuU can inject the required settings for various locales. Currently only German (DE), French (FR), Dutch (NL), English (UK) and English (US) are supported[2].

[2] Further enhancements to the number of supported locales will be made in subsequent releases.

Copyright © 2008 – 2013 Virtual Engine Limited

Figure 44 - PuU International Support



To load the relevant locale settings into the ***Registry Panel***, click the ***International*** button and select the required locale from the drop-down list. The resulting registry values will automatically be loaded into the ***Registry Panel***.

Updating Profiles

To merge registry information into the one or more user registry hives (profiles) you will need to select which registry (.REG) files you wish to merge and into which user profiles. To update profiles with registry (.REG) information perform the following steps:

1. Check each profile you want to update in the Profiles list. Every profile that is checked will be updated.
2. Check each registry file you want to merge into profiles selected in step 1. Each registry file that is checked will be merged into the selected profiles.
3. If you wish to inject the registry settings directly into the selected profiles without backing them up, select the ***Overwrite*** button in the toolbar.
4. If you wish to back up the selected profiles prior to injecting the registry changes, select the ***Backup*** button in the toolbar.
5. If you want the Profile Update Utility to delete any log files generated by REGEDIT, ensure that the ***Delete Logs*** option is enabled in the toolbar.
6. When you are ready to inject the selected registry files into all the selected profiles, click the ***Update*** toolbar button to begin the process.
7. View the ***Log*** tab in the reviewing panel to see a list of all the actions performed.

WARNING

If you select .REG files that have HKEY_LOCAL_MACHINE settings contained within then these will be merged into the Local Machine registry hive and not the mandatory profile!

Copyright © 2008 – 2013 Virtual Engine Limited

Job Execution Tool

The Virtual Engine Job Execution Tool (JET), JET Command Line (JETCMD) and JET Password (JETPWD) are separate tools for scheduling RES Automation Manager jobs without requiring direct access to the RES Automation Manager management console (WMC.EXE).

Combined, these tools overcome some shortcomings with unattended job scheduling in the RES Automation Manager product. Examples of where JET or JETCMD will help are:

- When scheduling a job unattended you have to specify the target agent that you wish a job to run on as there is no way to specify the "local" computer;
- When integrating RES Automation Manager jobs with RES Workspace Manager there is no provision to prompt the user for RES Automation Manager job parameters;
- When integrating RES Automation and RES Workspace Manager, jobs parameters can be used but they are defined by the administrator;
- When scheduling a RES Automation Manager job from the command line there is no way to specify job parameters without using a .CSV file.

JET

The main JET utility is a graphical interface, dynamically built from a XML configuration file that can invoke a single RES Automation Manager module, project or run book. Its initial intention was to be able to schedule RES Automation Manager jobs from a shortcut using parameters as this functionality is lacking in the RES Workspace Manager integration.

Typical uses can include invoking Active Directory object creation tasks for Helpdesk users. Without JET, helpdesk staff will need to be trained in how to use the RES Automation Manager console. JET can also be used during the imaging process to prompt for departments or application settings post deployment.

Installation

Whilst JET is installed on the machine that the Virtual Engine Toolkit is deployed on, the JET executable is a standalone executable that can be deployed or called from scripts or RES Automation Manager. Written in C# it does require the .Net Framework 4.0 to be installed.

The RES Automation Manager console (the RES Automation Manager console is required to schedule jobs from the command line) and RES Automation Manager agent need to be installed. If you attempt to launch JET without either the RES Automation Manager console or agent installed you will receive an error.

JET Configuration

JET requires two files to operate; the main standalone executable and a XML configuration file. By default JET will look for the ***JET.XML*** file in the directory the ***JET.EXE*** is running from. If the ***JET.XML*** configuration file is not found, you will receive an "Invalid XML file/format error."

Copyright © 2008 – 2013 Virtual Engine Limited

You can specify a configuration file when launching JET by passing the XML filename as a parameter. An example ***JET Customisation Demo.bat*** is included in the JET directory to demonstrate this functionality.

Here is a list of all supported options within the configuration file (an .XSD is also available in the JET installation directory):

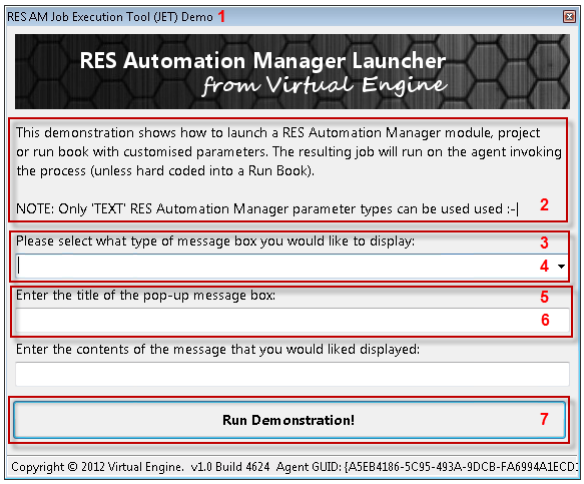
XML Tag	Description
<Title>	The title displayed in the JET window
<Description>	The introduction text
<Type>	**Required.** The target RES Automation Manager job type. Valid options are module, project or runbook.
<GUID>	**Required.** The target RES Automation manager job GUID.
<ButtonText>	The message/text to display on the JET button.
<HeaderFont>	The font to use in the header/description. Typical values are valid Windows system font names, i.e. Arial, Verdana or Calibri etc.
<HeaderBold>	Whether the header/description text is bold. Default value is ***false.***
<HeaderSize>	The font size of the header/description text. Default value is ***11.***
<BackColor>	The HTML colour code of the window. Default value is ***#FFFFFF.***
<HeaderImage>	The relative filename of the image to replace the default. The image needs to be located in the directory that JET is executed from.
<Username>	The RES Automation Manager username to authenticate with. By default, JET will attempt to authenticate with the local username/password.
<Password>	The RES Automation Manager password to authenticate with. By default, JET will attempt to authenticate with the local username/password.
<Encrypted>	Whether the <Password> supplied is encrypted with JETPWD. Default value is ***false***.
<Parameter>	**Required.** Used for each individual RES Automation Manager parameter.
<Name>	**Required.** The RES Automation Manager job parameter name. This must match the parameter name defined within the RES Automation Manager module, project or run book.
<Description>	**Required.** The text to display about the parameter textbox or drop down.
<Type>	**Required.** The type of object to display. Valid options are **Text** (text box) and **List** (drop down).
<ParameterValue>	**Required only for <TYPE>LIST</TYPE>.** Used to specify each drop down option for the specified parameter.

Copyright © 2008 – 2013 Virtual Engine Limited

<Value>	**Required only for <TYPE>LIST</TYPE>.** This is value that is passed to RES Automation Manager if this option is selected.
<Description>	**Required only for <TYPE>LIST</TYPE>.** This is value that is displayed in the drop down list.

JET supports customisation of the interface as well as the ability to define numerous parameters that the user is prompted for. Here is the default look-and-feel of the JET tool.

Figure 45 - JET Customisation Sample


RES AM Job Execution Tool (JET) Demo 1
RES Automation Manager Launcher
from Virtual Engine
This demonstration shows how to launch a RES Automation Manager module, project or run book with customised parameters. The resulting job will run on the agent invoking the process (unless hard coded into a Run Book).
NOTE: Only 'TEXT' RES Automation Manager parameter types can be used used :-| 2
Please select what type of message box you would like to display: 3
4
Enter the title of the pop-up message box: 5
6
Enter the contents of the message that you would liked displayed:
Run Demonstration! 7
Copyright © 2012 Virtual Engine. v1.0 Build 4624 Agent GUID: {A5EB4186-5C95-493A-9DCB-FA6994A1ECD3}

The configuration shown above has been generated from the XML below. For more examples, please refer to the JET installation directory for additional configuration samples.

Figure 46 – JET Configuration XML Sample

```
<?xml version='1.0' encoding='UTF-8'?>
<JETConfig>
	<Title>RES AM Job Execution Tool (JET) Demo</Title>
	<Description>This demonstration shows how to launch a RES Automation Manager module,
		project&#13;&#10;or run book with customised parameters. The resulting job will run
		on the agent invoking&#13;&#10;the process (unless hard coded into a Run
		Book).&#13;&#10;&#13;&#10;NOTE: Only 'TEXT' RES Automation Manager parameter types
		can be used used :-| </Description>
	<Type>runbook</Type>
	<GUID>{8BC1C0EA-FA11-4811-A4C9-0637720FD273}</GUID>
	<ButtonText>Run Demonstration!</ButtonText>
	<Parameter>
		<Name>MESSAGE_TYPE</Name>
		<Description>Please select what type of message box you would like to
			display:</Description>
		<Type>List</Type>
		<ParameterValue>
			<Value>INFO</Value>
			<Description>Informational Dialog</Description>
		</ParameterValue>
		<ParameterValue>
			<Value>WARN</Value>
			<Description>Warning Dialog</Description>
		</ParameterValue>
		<ParameterValue>
			<Value>ERR</Value>
			<Description>Error Dialog</Description>
		</ParameterValue>
	</Parameter>
	<Parameter>
		<Name>MESSAGE_TITLE</Name>
		<Description>Enter the title of the pop-up message box:</Description>
		<Type>Text</Type>
	</Parameter>
	<Parameter>
		<Name>MESSAGE_BODY</Name>
		<Description>Enter the contents of the message that you would liked
			displayed:</Description>
		<Type>Text</Type>
	</Parameter>
</JETConfig>
```

Note

Only 'TEXT' RES Automation Manager parameters types can be used!

Copyright © 2008 – 2013 Virtual Engine Limited

JETCMD

Complimentary to the Job Execution Tool GUI interface, there is also a command line version; JETCMD. It is more akin to a wrapper around the RES Automation Manager command line WMC.EXE.

WMC does not currently support several key options from the command line which JETCMD overcomes:

- Scheduling a job via WMC.EXE requires that you specify the target agent (or team) GUID. There is no way to schedule a job on the executing agent without knowing its GUID in advance;
- Parameters cannot be passed to a RES Automation Manager dispatcher without the use of a .CSV file. Therefore, it's difficult to pass parameter values via the command line.
- There is no way to pass an obfuscated password on the command line leaving RES Automation Manager credentials in clear view;
- RES Workspace Manager integration does not permit the scheduling of RES Automation Manager jobs as a logoff action.

Typical uses can include invoking a RES Automation Manager project or run book during OS deployment in the SetupComplete.cmd script or invoking RES Automation Manager jobs at logoff, i.e. to delete local profiles.

Installation

Whilst JETCMD is installed on the machine that the Virtual Engine Toolkit is deployed on, the JETCMD executable is a standalone executable that can be deployed or called from scripts or by RES Automation Manager. Written in C# it does require the .Net Framework 4.0 to be installed.

The RES Automation Manager console (the RES Automation Manager console is required to schedule jobs from the command line) and the RES Automation Manager agent only needs to be installed if you wish to schedule jobs on the local machine. If you attempt to launch JET without the RES Automation Manager console installed you will receive an error.

Usage

The command line options for JETCMD are fairly self-explanatory.

```
JETCMD.EXE /type:<Job Type> /jobguid:<Module GUID> /agent:<Agent GUID>
           [/user:<UserName>] [/password:<Password>] [/encrypted]
           [/paramname:<Parameter1,Parameter2..> /paramvalue:<Value1,Value2..>]

    /type       RES AM Job Type, i.e. module, project or runbook.
    /jobguid    RES AM module, project or runbook GUID to execute.
    /agent      RES AM agent GUID to run the job on. Use LOCAL for the
                  agent that JETCMD is invoking from.
    /user       RES AM console user to authenticate as. If this option is not
                  specified then pass-through authentication is used.
    /password   Password for the [/username] parameter (if specified).
    /encrypted  Specifies that the password supplied has been encrpyted.
    /paramname  Specifies parameter name(s) separated by commas (CSV)
    /paramvalue Used inconjuction with /paramname to specify the parameter value(s)
```

Copyright © 2008 – 2013 Virtual Engine Limited

Passing Parameters

Having stated that everything is fairly straight-forward, passing RES Automation Manager parameter values via the command line may require some additional clarification! There are some simple rules that need to be followed:

- If you have any spaces in either the parameter names or parameter values they need to be enclosed within quotation marks. For example, a parameter value for ***Hello World!*** needs to specified as ***/paramvalue:"Hello World!"***
- If you have any embedded commas, the parameter names or parameter values need to be enclosed within nested quotation marks. For example, a parameter value for ***Hello, World!*** needs to be specified as ***/paramvalue:"""Hello, World!"""***. This ensures that at least one set of quotation marks makes its way through the RES Automation Manager job!
- A rule of thumb suggests that each parameter name and parameter value pair should be enclosed between nested quotation marks, just to be safe. For example, ***/paramname:"""MESSAGETITLE""","""MESSAGEBODY""" /paramvalue:"""Job Successful""","""The target job has finished"""***

Note

Only 'TEXT' RES Automation Manager parameters types can be used! This is a restriction imposed by WMC.EXE and not of JETCMD.EXE itself.

Verbose Logging

There is a hidden ***/verbose*** command line switch that enables verbose output. With this switch, JETCMD will output each parameter name and parameter value passed in via the command line interpreter. This will potentially highlight any syntax errors if required.

Note

The /USER parameter only supports RES Automation Manager authentication and not Windows authentication!

Copyright © 2008 – 2013 Virtual Engine Limited

JETPWD

Both JET and JETCMD support the use of obfuscated passwords to ensure that passwords in JET XML configuration files or JETCMD references in scripts do not contain clear text passwords. To generate an encrypted password for either tool, the command line JETPWD tool must be used.

Installation

Whilst JETPWD is installed on the machine that the Virtual Engine Toolkit is deployed on, the JETPWD executable is a standalone executable that can be deployed or called from scripts or by RES Automation Manager. Written in C# it does require the .Net Framework 4.0 to be installed.

Usage

JETPWD usage is very simple. Run ***JETPWD.EXE <Clear Text Password To Encrypt>***. For example, ***JETPWD.EXE Password*** will generate the following output ***BkDgPOAJtGgyQeaHY+xhhA==***.

The encrypted password can now be embedded within a JET XML configuration file. Here is a sample snippet of a configuration XML file with an encrypted password:

```
<JETConfig>
	<Title>RES AM Job Execution Tool (JET) Demo</Title>
	<Description>Encrypted Password Example</Description>
	<Type>runbook</Type>
	<GUID>{8BC1C0EA-FA11-4811-A4C9-0637720FD273}</GUID>
	<ButtonText>Run Demonstration!</ButtonText>
	<Username>RES-AM-User</Username>
	<Password>BkDgPOAJtGgyQeaHY+xhhA==</Password>
	<Enrypted>true</Encrypted>
	<Parameter> ….
```

Using an encrypted password with JETCMD is also simple. The following command launches a RES Automation Manager run book on the local agent, using RES Automation Manager authentication:

```
JETCMD /type:runbook /jobguid:{8BC1C0EA-FA11-4811-A4C9-0637720FD273} /agent:local
/user:RES-AM-User /password:BkDgPOAJtGgyQeaHY+xhhA== /encrypted
```

Copyright © 2008 – 2013 Virtual Engine Limited

WSUS Integration Management Pack

The Virtual Engine WSUS Integration Management Pack (WiMP) is provided as a standalone executable. Its sole purpose is to automate the installation of Microsoft Windows Updates either directly from the Windows Update servers or via a WSUS server, on demand.

Microsoft's WSUS server and Group Policies are fantastic for patching client workstations and laptops. Unfortunately, this solution does not cater too well for server class machines.

Within a typical organisation, security officers would ideally like to patch its servers in a repeatable and predetermined order at an agreed date/time. In this theoretical ideal world, it would also be desirable to take into account the dependencies and interactions between various systems. For example, it's probably not a great idea to patch and reboot all Active Directory domain controllers or Citrix XenApp servers at exactly the same time (even if it is a Saturday!).

The native Microsoft Windows Update client and Group Policy Objects (GPOs) do not grant us this level of flexibility or granularity which can lead to deployment of 3rd party patch management tools, manual installations or no installations at all.

RES Automation Manager provides an excellent scheduling engine that is capable of handling the advanced run book functionality required to ensure that tasks are completed in a given order. Unfortunately, it does not have any native capacity to invoke the Windows Update client.

WiMP can be used to invoke and install approved Windows Updates (directly from Windows Update if a WSUS has not been configured). After the installation of any updates, the pending reboot status of the Windows Update client is also reflected in the registry. This process can allow RES Automation Manager (or any other automation tool) to determine whether a reboot is required and control this process.

WARNING

WiMP is currently at version 0.6 and therefore still considered a Beta release. Please ensure that you test this thoroughly in your environment!

Copyright © 2008 – 2013 Virtual Engine Limited

Installation

WiMP is installed as part of the Virtual Engine Toolkit in the <VET Install Dir>\WiMP directory. The WiMP.EXE file can be copied/deployed anywhere appropriate, and, as a standalone executable there is no additional installation required.

If RES Automation Manager integration is desirable there is a sample Building Block <VET Install Dir>\WiMP\WiMP v0.6.xml) supplied. All modules and project(s) are documented and have descriptions attached.

WiMP is not restricted to Microsoft Windows Server operating systems and will also work on workstation operating systems. The included project can be used to recursively patch any Windows operating system. This can be useful during Windows deployment processes to ensure the new OS is patched as quickly as possible.

Usage

WiMP usage is very simple:

```
Usage: WiMP.EXE [/scan] [/download]
   /scan      Only scans for missing (authorised) updates
   /download  Only scans and downloads missing (authorised) updates

If no command line arguments are supplied, WiMP will scan, download and
INSTALL all applicable/authorised updates from Windows Update or WSUS.

Exit Codes:

    0 - Successful, no reboot required
    1 - Successful, reboot required
    2 - Not scanned as reboot pending
    3 - Failed
```

If no command line switches are supplied then WiMP will scan, download **and install** all applicable/authorised Windows Update!

Reboots

If the Windows Update client signifies that a reboot is required, WiMP will set the HKLM\Software\Virtual Engine\WiMP\RebootPending (REG_DWORD) value to 1. If no reboot is required the RebootPending value will contain a value of 0.

Note

WiMP will not automatically approve updates or reboot a machine.

Copyright © 2008 – 2013 Virtual Engine Limited

Appendix A – Group Policy Migration

VET will migrate Group Policy Object links and security filtering into the RES Workspace Manager building block file(s) if instructed to do so. What follows is a detailed description on how these settings are converted and how they are implemented within RES Workspace Manager.

Security Filtering

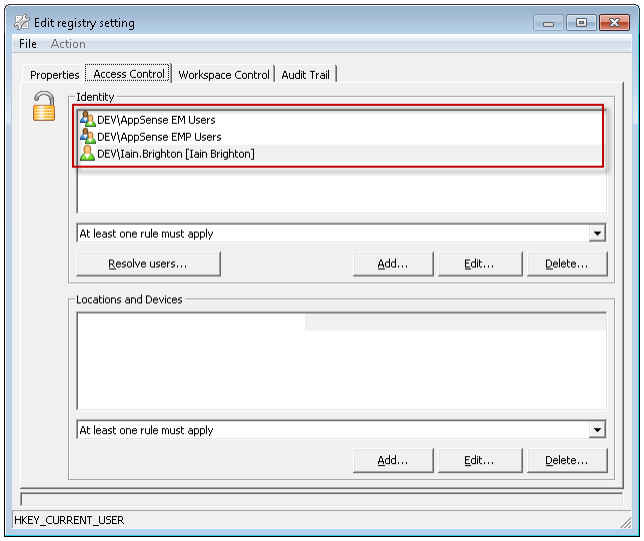
The ability for a Group Policy Object to be applied to a user (or computer) requires the Active Directory "Apply Group Policy" extended right to be assigned. By default, when a new GPO is created the built-in ***Authenticated Users*** group is given this right. If the ***Authenticated Users*** group is found on a GPO then VET will implement this as the RES Workspace Manager built-in ***All Users*** access principal.

WARNING

Delegation of rights is not migrated and therefore, any denied "Apply Group Policy" rights are not migrated as they cannot be implemented efficiently. They are however reported in the GPO summary report!

If ***Authenticated Users*** is not detected, then VET will migrate the users/groups that have the "Apply Group Policy" object right. These permissions are implemented in the RES Workspace Manager console under the ***Identity*** node.

Figure 47 - Migrated Security Filtering



Copyright © 2008 – 2013 Virtual Engine Limited

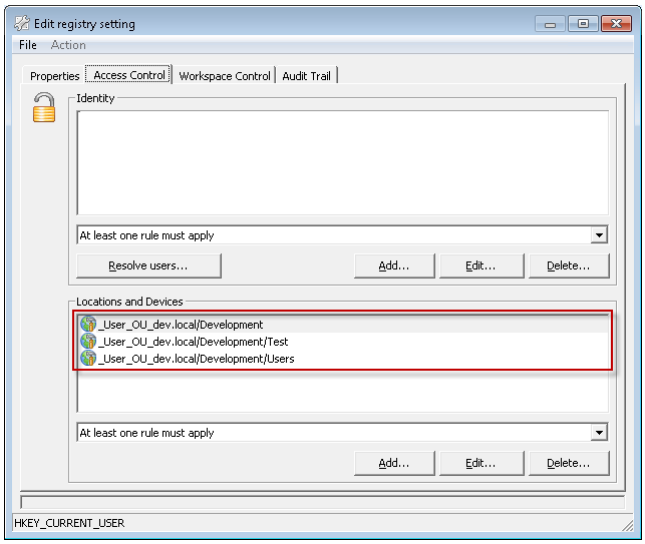
OU and Site Links

Active Directory OU and site links are implemented as RES Workspace Manager zones.

Note

Regardless of the status of the imported objects, the Active Directory OU and Site links will always be enabled.

Figure 48 - Migrated GPO Links



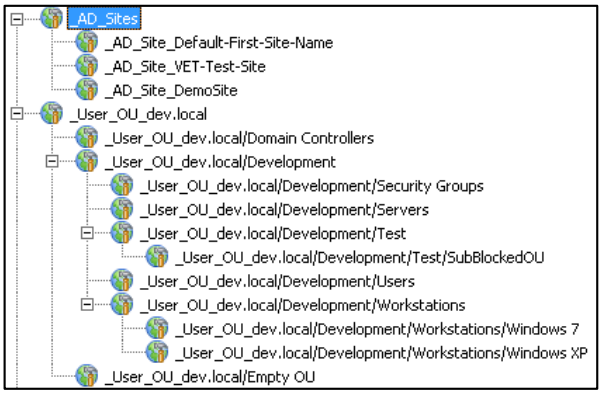
This might seem counterintuitive to be begin with, but there is a perfectly valid reason for this. A Group Policy Object can be linked to multiple Active Directory organisational units and/or multiple Active Directory sites. Natively, RES Workspace Manager supports targeting objects at an organisational unit level, but not sites.

Note

Combining Security Filtering rules and organisational links in the ***Identity*** node of the RES Workspace Manager console would also require multiple objects to be created to support the combination of permitted users/groups and OU links.

The sites and user OUs are created as zones with the _AD_Site_ and _User_OU_ prefixes to ensure that they're easily identifiable within the RES Workspace Manager console.

Figure 49 - RES Workspace Manager Zones



Copyright © 2008 – 2013 Virtual Engine Limited